

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059864

(43)Date of publication of application : 25.02.2000

(51)Int.Cl.

H04Q 7/38

H04B 7/15

H04B 7/26

H04M 15/00

(21)Application number : 11-133303

(71)Applicant : ICO SERVICES LTD

(22)Date of filing : 13.05.1999

(72)Inventor : HUI KELLY

(30)Priority

Priority number : 98 98305186

Priority date : 30.06.1998

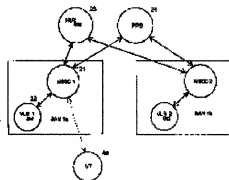
Priority country : EP

(54) PREPAID LONG DISTANCE COMMUNICATION METHOD AND DEVICE THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To attain improvement of security by deciding a time and a period of time during which a subscriber is permitted to use services on the basis of the amount of available credit.

SOLUTION: A prepaid server (PPS) 24 identifies a subscriber on the basis of international mobile subscriber's identity(IMS) information, retrieves a corresponding credit record, uses a destination network identity, dial number information and current time information, and decides a charge table applied to a call. The PPS 24 calculates a call period of time permitted to a specific call generated onto a network. This information is transmitted to a user terminal(UT) and a subscriber's identification module (SIM) by way of a home network MSSC 21 in a standard GSM unstructured supplementary service data(USSD) message. The SIM enables a call on a destination network 8 and instructs the UT to return to normal display. When the connection is established, the SIM activates an internal timer.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-59864

(P2000-59864A)

(43) 公開日 平成12年2月25日 (2000. 2. 25)

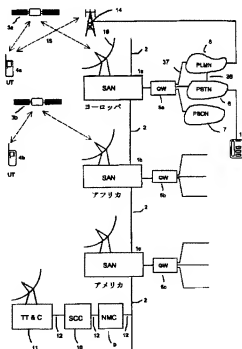
(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 H
H 0 4 B 7/15		H 0 4 M 15/00	G
7/26			Z
H 0 4 M 15/00		H 0 4 B 7/15	Z
		7/26	Z
		審査請求 未請求 請求項の数16 O L (全 13 頁)	
(21) 出願番号	特願平11-133303	(71) 出願人	597129263 アイシーオー・サーヴィシーズ・リミテッド
(22) 出願日	平成11年5月13日 (1999. 5. 13)		イギリス・W 6・9 B N・ロンドン・クイーン・キャロライン・ストリート・1
(31) 優先権主張番号	9 8 3 0 5 1 8 6 . 3	(72) 発明者	ケリー・ヒュー
(32) 優先日	平成10年6月30日 (1998. 6. 30)		イギリス・W 6・9 B N・ロンドン・クイーン・キャロライン・ストリート・1・シー・オー・アイシーオー・サーヴィシーズ・リミテッド
(33) 優先権主張国	ヨーロッパ特許庁 (E P)	(74) 代理人	100064908 弁理士 志賀 正武 (外 9 名)

(54) 【発明の名称】 料金前払遠距離通信方法および装置

(57) 【要約】

【課題】 加入者のクレジット情報を使用者端末へ送信する必要が無く、その結果、保安性に優れた料金前払遠距離通信方法および装置を提供すること。

【解決手段】 衛星移動電話システムへの料金前払加入者は、移動先地上ネットワーク上で、他の全ての加入者と同じサービスを提供される。加入者ネットワークは、各料金前払加入者に対するクレジット記録を保持し、かつ、加入者の利用可能なクレジットが（他のネットワーク上で）許可する呼時間の最大量を（他のネットワーク上のサービスにアクセスすることを求める加入者の使用者端末からの要求に応じて）計算することができる。利用可能な呼時間は、使用者端末へ送信される。該使用者端末は、経過していない呼時間を第1ネットワークへ通知するだけでなく、呼を制御する。



【特許請求の範囲】

【請求項 1】 第 1 通信ネットワークへの料金前払加入者が第 2 通信ネットワークへ移動するときに、該加入者に対して、第 2 通信ネットワークによって提供される通信サービスへのアクセスを提供する方法であって、加入者は、該サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、サービスをすることを加入者が許可される時間期間を、利用可能なクレジット量に基づいて決定し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする方法。

【請求項 2】 請求項 1 記載の方法において、加入者が第 2 ネットワークへ移動している間に、第 1 ネットワークで時間期間を決定することを具備することを特徴とする方法。

【請求項 3】 請求項 2 記載の方法において、第 1 ネットワークに接続された計算手段で時間期間を決定することを具備することを特徴とする方法。

【請求項 4】 請求項 2 記載の方法において、加入者は、使用者端末を介して、サービスにアクセスでき、サービスへのアクセスに対する使用者端末からの要求に応じて時間期間を決定することを具備することを特徴とする方法。

【請求項 5】 請求項 3 記載の方法において、加入者がサービスにアクセスしている使用者端末へ、計算手段から、予め決定された時間期間の送信を開始することを更に具備することを特徴とする方法。

【請求項 6】 請求項 4 記載の方法において、専有の信号フォーマットを使用した使用者端末への送信のために、予め決定された時間期間を符号化することを具備することを特徴とする方法。

【請求項 7】 請求項 1 記載の方法において、第 1 ネットワークは、衛星遠距離通信ネットワークを具備し、かつ、第 2 ネットワークは、地上ベースの移動ネットワークを具備することを特徴とする方法。

【請求項 8】 第 1 通信ネットワークへの料金前払加入者が第 2 通信ネットワークへ移動している間に、該加入者に対して、第 2 通信ネットワークによって提供される通信サービスへの使用者端末を介したアクセスを提供する方法であって、

加入者は、該サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、加入者によって利用可能なクレジットの量に対応するサービスを使用することを加入者が許可される時間期間の決定を要求する送信を、使用者端末から第 1 ネットワークへ開始し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする方法。

【請求項 9】 請求項 8 記載の方法において、時間期間決定要求が生成されることを可能とするために、使用者端末によって生成される呼を禁止することを具備することを特徴とする方法。

【請求項 10】 請求項 8 記載の方法において、予め決定された時間期間の通知を受信することを具備することを特徴とする方法。

【請求項 11】 請求項 8 記載の方法において、現在起こっている呼の期間を予め決定された時間期間と比較することを具備することを特徴とする方法。

【請求項 12】 請求項 10 記載の方法において、予め決定された時間期間が終了すると、サービスを使用して使用者端末によって生成された呼を終了することを具備することを特徴とする方法。

【請求項 13】 請求項 8 記載の方法において、サービスを使用して使用者端末によって生成された呼が終了された後、時間期間の送信を第 1 ネットワークへ開始することを具備することを特徴とする方法。

【請求項 14】 第 1 ネットワークと第 2 ネットワークとを具備する遠距離通信ネットワーク構成であって、該ネットワーク構成は、第 1 ネットワークへの料金前払加入者が第 2 ネットワークへ移動するときに、該加入者に対して、第 2 ネットワーク上の通信サービスへのアクセスを提供し、

加入者は、前記サービス上での使用に対して利用可能な予め決定されたクレジット量を有し、サービスを使用することを加入者が許可される時間期間を、利用可能なクレジット量に基づいて決定するためのプロセッサを更に具備し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする遠距離通信ネットワーク構成。

【請求項 15】 請求項 14 記載のネットワーク構成において、プロセッサは、第 1 ネットワークに接続された料金前払サーバーを具備することを特徴とするネットワーク構成。

【請求項 16】 第 1 通信ネットワークへの料金前払加入者が第 2 通信ネットワークへ移動するときに、該加入者に対して、第 2 通信ネットワーク上の通信サービスへの使用者端末を介したアクセスを提供する装置であって、加入者は、前記サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、サービスを使用することを加入者が許可される時間期間を、クレジット量に基づいて決定するために、使用者端末からの要求に応答するプロセッサを具備し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、移動遠距離通信ネットワークにおける料金前払遠距離通信サービスの設備に関する。この発明は、特に、自身のホームネットワークから離れた移動している料金前払加入者へ料金前払遠距離通信サービスを提供することに關するが、このことのみに関するわけではない。

【0002】

【従来の技術および発明が解決しようとする課題】地上移動遠距離通信システムはよく知られており、かつ、(異なる規格に従って動作する)多数の異なるシステムが開発されている。これらの公衆地上移動ネットワーク(PLMN)は、アナログ規格またはデジタル規格に従って動作する。ヨーロッパほとんどの極東と他の地域とは、グローバルシステムモバイル(Global System Mobile: GSM)ネットワークが普及している。一方、合衆国では、アドバンスドモバイルフォンサービス(Advanced Mobile Phone Service: AMPS)およびディジタルアドバンスドモバイルフォンシステム(Digital Advanced Mobile Phone System: DAMPS)が使われており、かつ、日本では、パーソナルハンディフォンシステム(Personal Handphone System: PHS)およびパーソナルディジタルコミュニケーション(Personal Digital Communication: PDC)ネットワークが使用されている。より最近では、世界的な移動遠距離通信システム(UMTS)についての提案がなされている。これらのネットワークは、全て、(移動使用者端末と通信する)送信機/受信機を伴うセルラーネットワークおよび地上ベースのネットワークである。

【0003】例えば、GSMシステムに基づくPLMNでは、PLMNの個々のセルは、地理的に間隔をあけられた一連の地上基地トランシーバ局(BTS)によって処理されている。BTSは、基地局コントローラ(BSC)を通して、移動スイッチングセンター(MSC)へ結合されている。MSCは、ネットワークから従来の公衆交換電話ネットワーク(PSTN)へのゲートウェイを提供する。PLMNは、ホームロケーションレジスタ(HLR)を具備する。HLRは、システムへの加入者とか加入者の使用者端末とに関する情報を記憶する。一般的に、GSMの顧客は、単一のPLMN(ここでは、「加入者のホームネットワーク」として参照する)との契約関係を有する。使用者端末がスイッチを入れられると、該使用者端末はホームネットワークのHLRに自己を登録する。もし、使用者が別のGSMネットワークへ移動すると、使用者端末は、訪問先ネットワークのビジターロケーションレジスタ(VLR)に自己を登録する。訪問先ネットワークは、認証および経路指定および他の目的のために、ホームネットワークのHLRと通信する。DAMPSネットワークおよびPHSネット

ワークおよびPDCネットワークは、類似のロケーションレジスタを有する。

【0004】より最近では、移動使用者端末と従来の地上ネットワークとの間における衛星通信リンクを使用する多数の異なる移動遠距離通信システムが提案されている。

【0005】あるネットワークは、いわゆる低地球軌道(LEO)衛星の一群を使用する。該低地球軌道衛星は、780kmの軌道半径を有する。該ネットワークは、イリジウム(登録商標)衛星セルラーシステムとして知られ、かつ、例えば、欧州特許公開第036585号公報および米国特許第5394561号公報(モトローラ)に記載されている。電話送受器のような移動使用者端末は、頭上の軌道周回衛星へのリンクを確立する。呼は、該軌道周回衛星から、(衛星群内の)他の衛星へ、そして、一般的には(従来の地上ベースのネットワークへ接続されている)地上局へ、送信されることが出来る。

【0006】他の案が提案されている。該案は、いわゆる中間地球軌道(MEO)衛星群を使用する。該中間地球軌道衛星は、10000~20000kmの範囲の軌道半径を伴う。Walker J.G. による"Satellite Patterns for Continuous Multiple Whole Earth Coverage"(1997年、Royal Aircraft Establishment)の第119~122頁目を参照された。さらに、例えば、英国特許公開第2295296号公報に記載されているICO(登録商標)衛星セルラーシステムと、欧州特許公開第0510789号公報に記載されているオデッセイ(登録商標)衛星セルラーシステムとを参照されたい。これらのシステムでは、衛星通信リンクは、隣接する衛星間における通信を許可しない。代わりに、(移動送受器のような)移動使用者端末からの信号は、最初に衛星へ送信され、そして、地上局(即ち、衛星アクセスノード: SAN)へ送信される。SANは、従来の地上ベースの電話ネットワークへ接続されている。このことは、「システムの多くの構成要素は(GSMのような)既知のディジタル地上セルラーテクノロジーと互換性がある」という利点を有する。また、LEOネットワークを伴う場合よりもより簡単な衛星通信技術が使用されることが出来る。

【0007】衛星通信ネットワークでは、軌道周回衛星と通信するために、地上局が、世界の色々な場所に配置されている。ICO(登録商標)システムおよび他のシステムでは、ビジターロケーションレジスタが、各々の衛星地上局と関連付けられている。該衛星地上局は(個々の地上局を使用している)個々の使用者端末の記録を保持する。

【0008】世界のあるエリアでは、従来の地上PLMNによって提供される受信可能範囲と衛星ネットワークによって提供される受信可能範囲とが重なることがあ

る。「個々の使用者端末が地上PLMNまたは衛星ネットワークのいずれかを伴って選択的に動作する」ということが提案されている。使用者端末は、使用者がネットワークを選択することを許可するためのスイッチを具備してもよく、他には、(例えば、定義された顧客の選択または他の要因に基づいて)自動的選択が行われてもよい。故に、例えば、ICD加入者は、(加入者への課金のために)課金情報および他の待遇情報がICDシステムへ送り戻されながら、PLMNを移動先ネットワークとして使用できる。「通常、費用および信号強度を含む理由のために、(例えば、市街地において)利用可能の時は、従来の地上PLMNが好まれる」ということが予測される。

【0009】他のネットワークへ移動した加入者によるネットワークの使用は、関係するネットワークオペレータ間の移動契約によって管理される。これらの契約は、一般的に、料金表情報の包括的な交換について準備する。それによって、各ネットワークは、移動加入者によって負われるであろう費用を前もって計算できる。例えば、移動契約は、「移動先ネットワークBが、(特定の位置へ電話をかけている)ホームネットワークAの加入者に対して、特定の料金表で、(例えば、移動先ネットワークBが該移動先ネットワークBの加入者に請求する額に15%をプラスした額に等しい)移動レートで請求する」ということを提供する。

【0010】ネットワークAの加入者がネットワークBへ移動すると、ネットワークBは、初めに、ネットワークAを用いて加入者を認証することを要求する。もし、ネットワークAが必要な認証を提供するならば、加入者は、ネットワークBを使用して電話をかけることを許可される。このことは、適切な比率で、該呼に料金請求する。そして、該呼に対する請求者が(一般的に、予め決定された期間に渡ってネットワークAの全ての加入者へネットワークBによって提供されたサービスに対して総計された料金の一部として)加入者のホームネットワークAへ送られる。そして、ホームネットワークAのオペレータは、ホームネットワークAの加入者それぞれに課金することができる。GSMシステムでは、例えば、該料金請求手続は、(各呼に対して生成され、かつ、使用料クレジットとして知られる)個々の記録または呼詳細記録に基づく。この原理は、呼を送る際に多数のネットワークが関係する場合に速やかに拡張する。

【0011】通常の経過時間に基づいて(呼に対して)料金請求するだけでなく、多くのオペレータは、該オペレータ自身の加入者に対して料金前払サービスを提供している。該サービスでは、加入者は、指定された量の呼時間に対して、前もって支払いを行う。多くの加入者にとって、呼費用を制御することを補助するという魅力ある選択であるだけでなく、料金前払サービスは、衛星電話システムのオペレータに対する特に重要な料金請求の

形式である。該オペレータにとって、料金前払システムは、該サービスがカバーする多くの国(特に、現金ベースの経済を有する国、または、適切なクレジット照合設備のない国)において支払いを補償する唯一の方法である。

【0012】しかしながら、料金前払加入者に移動可能性を提供することに関連して、重大な困難が存在する。実例としては、訪問先ネットワークBがネットワークAの移動料金前払加入者の内の1人を認証しようとする場合、もし「加入者が該加入者に割り当てられたクレジットを越えて使用しない」ということを保証する方法が何もないならば、ネットワークAはそのような認証を提供しない。実際には、このことは、呼時間に対する支払いが一度失効すると、加入者の呼をリアルタイムで終了するいくつかの手段を要求する。

【0013】GSMネットワークに関して、この問題を解決する1つの可能な方法は、標準GSMアドバイソブチャージ(advice of charge:AOC)サービスを使用することである。該サービスでは、料金請求情報は、訪問先ネットワークBから移動使用者端末へ、(移動契約において指定される)料金表契約に基づいて送られる。例えば、呼のセットアップ時に、訪問先ネットワークBは、適用されるべき料金表を決定するために、料金分析機能を実行する。この料金表は、呼の開始時に、料金請求アドバイソブチャージ(charge advice information:CAl)構成要素の形式で、使用者端末へ送信される。該形式は、料金表を、単位料金や単位長等の点で記載している。CAlの受信時には、使用者端末は、実際の呼料金を計算し、かつ、該呼料金を、使用者端末内の加入者識別モジュール(SIM)に記憶された数値値から減算する。SIMは、利用可能なクレジット情報も記憶している。故に、使用者端末は「利用可能なクレジットが越えられない」ということを保証できる。

【0014】このアプローチの1つの欠点は、「料金請求情報が電波伝送媒体上を使用者端末へ標準AOCフォーマットで周期的に送信される」ということである。このことは、使用者端末/SIMインターフェースにおける(無料電話をかけるための)改竄の危険性を助長する。

【0015】他の欠点は、「もし、呼が多数のネットワーク上を移動料金前払加入者から経路決定されるべきならば、各ネットワークは、ホスト役のネットワークが正確なリアルタイム料金請求情報を移動加入者に提供できるように、ホスト役のネットワーク自身の移動料金表に基づいて、ホスト役のネットワークに、リアルタイムの料金請求情報を提供しなくてはならない」ということである。このことは、標準移動契約に渡りかつ該標準移動契約上において、関連する全てのネットワークオペレータの間における複数の相互的な契約を要求する。さらに、(このことによって生じる)潜在的な国際的ネット

7

ワーク上でのリアルタイム信号送信における実質的な増加は、「料金前払加入者へ移動能力を提供するという問題に対して、AOCアプローチが実際には実用的な解決でない」ということを意味する。

【0016】(リアルタイム料金請求情報が電波送信媒体インターフェース上を送信される)料金前払システムは、R. Krayem-Nevoux, G. Mazziotto, P. Hilleによる"Payphone Service for Third Generation Mobile Systems" (1993年 IEEE, XP-002088065) に開示されている。この文献は、「PLMNと使用者端末との間において電波送信媒体インターフェースを介して送信される構成要素に関する料金請求情報は、変造事実を両者(PLMNおよび使用者端末)に知られることなしに変造されることができない」ということを保証するために必要な保安特徴を記載する。

【0017】本発明は、上記欠点を除去する事を目的とする。

【0018】

【課題を解決するための手段】本発明によると、第1通信ネットワークへの料金前払加入者が第2通信ネットワークへ移動するときに、該加入者に対して、第2通信ネットワークによって提供される通信サービスへのアクセスを提供する方法であって、加入者は、該サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、サービスを使用することを加入者が許可される時間期間を、利用可能なクレジット量に基づいて決定し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする方法が提供される。

【0019】本発明による方法は、加入者が第2ネットワークへ移動している間に、第1ネットワークで時間期間を決定することを経験してもよく、このことは、第1ネットワークに接続された計算手段で時間期間を決定することを経験する。

【0020】本発明の更なる特徴によると、第1通信ネットワークへの料金前払加入者が第2通信ネットワークへ移動している間に、該加入者に対して、第2通信ネットワークによって提供される通信サービスへの使用者端末を介したアクセスを提供する方法であって、加入者は、該サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、加入者によって利用可能なクレジットの量に対応するサービスを使用することを加入者が許可される時間期間の通知を要求する送信を、使用者端末から第1ネットワークへ開始し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする方法が提供される。

【0021】本発明によると、第1ネットワークと第2ネットワークとを具備する遠距離通信ネットワーク構成であって、該ネットワーク構成は、第1ネットワークへ

8

の料金前払加入者が第2ネットワークへ移動するときに、該加入者に対して、第2ネットワーク上の通信サービスへのアクセスを提供し、加入者は、前記サービス上での使用に対して利用可能な予め決定されたクレジット量を有し、サービスを使用することを加入者が許可される時間期間を、利用可能なクレジット量に基づいて決定するためのプロセッサを更に具備し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする遠距離通信ネットワーク構成もまた提供される。

【0022】本発明によると、第1通信ネットワークへの料金前払加入者が第2通信ネットワークへ移動するときに、該加入者に対して、第2通信ネットワーク上の通信サービスへの使用者端末を介したアクセスを提供する装置であって、加入者は、前記サービス上での使用に対して利用可能な予め決定された量のクレジットを有し、サービスを使用することを加入者が許可される時間期間を、クレジット量に基づいて決定するために、使用者端末からの要求に応答するプロセッサを具備し、それによって、予め決定された時間期間に依存して、加入者による前記サービスの使用の制御が可能であることを特徴とする装置が更に提供される。

【0023】本発明の実施形態から得られる利点は、「ホームネットワークが、移動先ネットワークにとって明白な方法で、呼に対する制御を保持でき、故に、このことは、ネットワークオペレータ間における相互の契約に対する必要を除去する」ということである。この場合、移動先ネットワークは「処理されている加入者が料金前払加入者である」ということを知らず、そのため、呼の費用とクレジット情報とは、使用者端末へ送信される必要がない。このことは、ネットワークと加入者の保安を強化する。特に、加入者のクレジット情報は、ホームネットワークの単独制御下で保持でき、かつ、たとえ、クレジット情報に対応する呼時間情報が、使用者端末へおよび使用者端末から(本発明の実施形態に従って)送信されるとしても、この送信は、ホームネットワークに専有されるフォーマットで行われ、さらに追加の保安を提供する。

【0024】

【発明の実施の形態】本発明の実施形態が、一例として、添付図面を参照して、ここで説明される。添付図面は以下の通りである。図1は、本発明による衛星遠距離通信システムの概要図である。該衛星遠距離通信システムは、局所的な地上ベースの移動遠距離通信システムを伴う。図2は、SANTaの付近における衛星ネットワークおよび関連する地上セラーネットワークのより詳細なブロック図である。図3は、衛星ネットワーク内の料金前払サーバーの設備を分解する概要ブロック図である。図4は、移動使用者端末の概要図である。図5は、図4に示される使用者端末の回路の概要ブロック図であ

る。図6は、図4および図5に示されるSIMカードの概要ブロック図である。図7は、本発明によるクレジット照合手続を示すフローチャートである。

【0025】図1を参照すると、衛星移動電話システムは、複数の衛星アクセスノード(SAN) 1a, 1b, 1cと、複数の衛星3a, 3bと、複数の使用者端末(UT) 4a, 4bと、ゲートウエイ(GW) 5a, 5b, 5cと、ネットワーク管理センター(NMC) 9と、衛星制御センター(SCC) 10と、追跡・遠隔測定・制御局(TT&C) 11とを具備する。複数のSAN 1a, 1b, 1cは、高容量デジタルネットワーク2(バックボーンネットワーク)によって相互結合されている。GW 5a, 5b, 5cは、SAN 1a, 1b, 1cと他の従来の地上ベースの電話ネットワーク6, 7, 8との間の接続を提供する。NMC 9とSCC 10とTT&C 11とは、低容量デジタルネットワーク12によって相互結合されている。低容量デジタルネットワーク12は、また、バックボーンネットワーク2へ接続されている。他の地上ベースの電話ネットワーク6, 7, 8は、公衆交換電話ネットワーク(PSTN) 6と公衆交換データネットワーク(PSDN) 7と公衆地上移動ネットワーク(PLMN) 8を含む。PSTN 6は、従来の電話器13への接続が成されることを可能とする。

【0026】SCC 10とTT&C 11とは、衛星3a, 3bの動作(例えば、送信電力レベルの設定とトランスポンダー入力の同調)を、NMC 9による図9の通りに制御する。衛星3a, 3bからの遠隔測定信号は、「衛星3a, 3bが正確に機能している」ということを保証するために、TT&C 11によって受信され、かつ、SCC 10によって処理される。

【0027】図1に示されるように、使用者端末UT 4aは、また、従来の地上ベースの移動ネットワークPLMN 8と通信できる。PLMN 8は、(使用者端末UT 4aとの二重通信方式リンク15を確立する)トランシーバ局14を具備する。この例では、PLMN 8は、GSMネットワークである。

【0028】GSMのより完全な理解のためには、欧州遠距離通信学会(ETSI)によって発行されている様々なGSM勧告を参照されたい。より読みやすい概観としては、M. MoulyとM-B. Pautetとによる「The GSM System for Mobile Communications」(1992年、Cell & Sys, ISBN:2-9507190-0-7)も参照されたい。

【0029】衛星ネットワークは、世界中に及ぶ受信可能範囲を提供するように設計されている。そのため、衛星3a, 3bは、衛星群の一部を形成する。該衛星群は、いくつかの軌道内に配置されている。一例では、5つの衛星の2つの軌道が使用される。これらの衛星は、地球の表面の大部分の受信可能範囲を提供するように示されることができる。該受信可能範囲では、10°の衛星上昇角度に対して、1つの衛星が、UTによ

て、全ての時間においてアクセスされることができ、かつ、2つの衛星が、少なくとも80%の時間に渡って、アクセスされることができる。その結果、システムの多様性を提供する。追加の冗長性と多様性を提供するために、更なる衛星が衛星群内に具備されてもよい。

【0030】本発明は、特定の軌道半径に限定されるものではないが、衛星は、(例えば、10355 kmの軌道半径を有する)中間地球軌道(MEO)群内に配置されている。この実施形態では、衛星3a, 3bは、共通の軌道内に示されており、かつ、該衛星は、各SAN 1a, 1b, 1cのアンテナ配列16によって追跡される。一般的に、各SANは、衛星群の個々の衛星を追跡するために4つのアンテナ(と1つの予備アンテナ)を具備する。SANは、連続した受信可能範囲を提供するために、地球の方々に間隔をあけて置かれている。示された実施形態では、SAN 1aはヨーロッパに配置されており、一方、SAN 1bはアメリカに配置されており、かつ、SAN 1cはアメリカに配置されており、かつ、他のSANは他の場所に配置されている。図1では、SAN 1bは、衛星3bを介して使用者端末UT 4bと通信していることが示されている。衛星ネットワークの更なる詳細については、英国特許公開第2295296号公報を参照されたい。

【0031】衛星3a, 3bは、非静止軌道内に存在し、かつ、ヒューズ(Hughes)HS 601のような従来の衛星を一般に具備する。該衛星3a, 3bは、英国特許公開第2288913号公報に記載されているような特徴を具備してもよい。各衛星3a, 3bは、衛星の下の(地球上の)フットプリントをカバーする無線ビームの配列を生成するように配置されている。各ビームは、英国特許公開第2293725号公報に記載されているように、多数の異なる周波数チャネルおよびタイムスロットを具備する。故に、該ビームは、隣接するセルラエリアを提供する。該セルラエリアは、従来の地上ベースの移動電話ネットワークのセルに対応する。

【0032】電話呼の間、使用者端末UT 4a, 4bは、(ダウンリンクチャネルとアップリンクチャネルとを具備する)全二重通信方式チャネルを介して、衛星3a, 3bと通信する。該チャネルは(呼の開始時に割り当てられた周波数上または呼の間に再割り当てされた周波数上)TDMAタイムスロットを具備する。

【0033】図2を参照すると、SAN 1aおよび(局所的な)PLMN 8の構成が、より詳細に示されている。SAN 1aは、衛星基地局BS 20からなる。BS 20は、衛星を追跡するための5つの直状アンテナ16へ結合されている。BS 20は、増幅器とマルチプレクサとデマルチプレクサと符号器とを伴う送信/受信回路を具備する。移動衛星スイッチングセンターMSSC 21は、BS 20へ結合されており、かつ、衛星ビジターロケーションレジスタVLR SAT 22を具備

する。MSSC 21は、通信信号を、バックボーンネットワーク2およびSBS 20へ結合する。それによって、個々の電話呼が(バックボーンネットワーク2および二重通信方式リンクを通して、衛星3aを介して)移動端末UT 4aへ確立されることを可能とする。

【0034】また、MSSC 21は、(図1に示されるPSDN7およびPSTN6) PLMN8への出力接続を提供するために、ゲートウエーGW 5aへ接続されている。「全てのSANは、登録されている加入者の記録を保持するために、個々のVLR SATを伴う類似の構成である」ということが理解される。

【0035】VLR SAT 22は、現在登録されている各々の加入者の記録(即ち、信号通信のためにSAN 1aを使用している各使用者の同一性)を保持する。

【0036】MSSC 21は、信号を該信号の目的地へ適切に送るために、アンテナ16からの到来通信信号上のアドレスに応答する。

【0037】図3を参照すると、衛星サービス設備は、データベースを使用する。該データベースは、ここでは、衛星ホームロケーションレジスタ(HLR SAT) 23として参照される。HLR SAT 23は、各移動ユーザーに関する契約記録を具備する。該記録は、使用者の同一性を含む。該同一性は、国際的移動加入者アイデンティティ(International Mobile Subscriber Identity: IMSI)と、契約の現在状態と、UTの現在の登録位置とを含む。HLR SATは、(図1に示される)NMC 9に配置されてもよく、または、SAN 1a、1b、1c内に分散配置されてもよい。

【0038】衛星サービス設備は、また、サーバーを使用する。該サーバーは、ここでは、料金前払サーバー(PPS) 24として参照される。PPS 24の動作は、以下に詳細に説明される。HLR SATを伴うので、PPS 24の位置は、融通がきく。例えば、PPS 24は、(図1に示される)NMC 9に配置されてもよく、または、SAN 1a、1b、1cの内の1つに配置されてもよい。

【0039】図2を再び参照すると、この例におけるPLMN 8は、UKベースのGSMネットワークを具備し、かつ、多数の基地トランシーバ局BTS 30、31、32を具備する。BTS 30、31、32は、それ自体がよく知られた方法でセルラーネットワークをサポートするために、地理的に間隔をあけて配置されている。BTS 30は、関連するアンテナ14を伴って示されている。該アンテナ14は、地上線によって、基地局コントローラBSC 33へ接続されている。「複数のBTS 30、31、32が、それ自体がよく知られた方法でBSC 33へ接続されている」ということが理解される。BSC 33は、移動スイッチングセンターMSC 34へ接続されている。MSC 34は、移動ネットワーク内の呼を経路決定できる。また、MSC 34は、該呼

を、それ自体がよく知られた方法で、ゲートウエーGMSC 35を通して、線36上で、従来のPSTN 6へ送ることができる。または、MSC 34は、該呼を、線37上で、ゲートウエーGW 5aを通して、衛星ネットワークへ送ることができる。

【0040】地上ベースのネットワーク8に対するホームロケーションレジスタHLR 38は、GMSC 35へ結合されて提供される。従来の方法では、HLRは、ネットワーク8に加入している使用者のIMSIの記録を保持する。ビジターロケーションレジスタVLR 39は、ネットワーク8に一時的に登録された加入者の記録を保持する。例えば、UKに位置するPLMN 8では、他の国(例えば、ドイツ)内のGSMネットワークへの加入者は、UK内にいる間、一時的に、局所的に登録される。従来の方法では、電話使用情報は、VLR 39およびGMSC 35から、ドイツのネットワーク(不図示)へ、課金目的のために中継される。他のタイプのネットワークへのPLMNの相互連結は、インターワーキングファンクション(Interworking function) IWF 40の設備によって、容易にされる。IWF 40は、GSM送信特性を、接続されたネットワークの送信特性に適合させるよう、構成されている。GSMのPLMNと衛星移動電話システムとの間におけるIWFの実行の詳細については、我々(出願人)の係争中の出願973022 22.1" Interworking between Telecommunications Networks"を参照されたい。

【0041】図4および図5を参照すると、移動使用者端末UT 4aは、局所的な地上セルラーネットワークおよび衛星ネットワークの両方を作った動作のように構成されている。故に、図2に示される例では、UT 4aは、地上ベースのGSMプロトコルと衛星ネットワークプロトコルとのいずれかに従って動作する。図4に示されるように、UT 4aは、移動送受器を具備する。該移動送受器は、デュアルモード動作が可能である。該移動送受器は、地上ベースのセルラーネットワークを作った使用のための従来のGSM回路を、衛星ネットワークを作った使用のための類似回路と共に、具備する。図4に示されるように、送受器は、マイクロフォン50とラウドスピーカ51とバッテリー52とキーパッド53とアンテナ54とディスプレイ55とを具備する。携帯装置UT 4aは、また、加入者識別モジュール(SIM) 56を具備する。SIM 56は、よく知られたサイズ(クレジットカードサイズ)を有するスマートカードであってもよく、または、ISO規格に従ったより小さなプラグインモジュールであってもよい。UT 4aの回路構成は、図5において、ブロック図形式で示される。SIM 56(例えば、SIMスマートカード)は、SIMカードリーダー57内に収納される。SIMカードリーダー57は、コントローラ58(一般的には、マイクロプロセッサ)に結合されている。マイクロフォン50

およびラウドスピーカー 51 は、第1符復号器 59 a および第2符復号器 59 b に結合されている。第1符復号器 59 a および第2符復号器 59 b は、従来の無線インターフェース 60 に結合されている。無線インターフェース 60 はアンテナ 54 に結合されている。それによって、通信信号を(本質的によく知られた方法で)送受信する。フェーズ 2+ compliant GSM システム

(Phase 2+ compliant GSM system) において、SIM 56 は、SIM アプリケーションツールキット (SIM Application Toolkit) として知られるソフトウェアを具備する。SIM アプリケーションツールキットは、SIM による (UT 機能の) 洗練された制御を可能にする。

【0042】図6を参照すると、SIM 56 は、メモリ M1 を具備する。メモリ M1 は、IMS I を記憶する。IMS I は、GSM ネットワーク 8 と衛星ネットワークとの両方で使用される。該メモリは、また、上記 GSM 動作に従う契約認証と通信暗号化のために、暗号化アルゴリズムと認証アルゴリズムと暗号化キー K1 とを記憶する。故に、UT 4 a は、(この技術分野でよく知られた) 従来の GSM 登録技術に従って、いずれのネットワークにも自己を登録できる。該認証手続および(その後) データの暗号化/解読の更なる詳細については、M. Mouly と M.-B. Pautet とによる "The GSM System for Mobile Communications" (1992年、Cell & Sys) の第477〜492頁目を参照されたい。

【0043】先に述べられたように、衛星ネットワークおよび地上ベースのネットワークは、使用者によって決定された基準に従って、自動的に選択される。しかしながら、この例では、説明を簡単にするために、衛星ネットワークおよび地上ベースのネットワークは、キーパッド 53 上のキーの使用によって、手動で選択される。GSM ネットワークが選択されると、コントローラ 58 は、無線インターフェース 60 を、地上ベースの GSM ネットワーク 8 に対して適切な周波数で動作するように設定し、かつ、(GSM ネットワークに対して適切な) 符復号器 59 a が選択される。他に、もし、衛星ネットワークを選択するようにキーパッド 53 が操作されたならば、コントローラ 58 は、無線インターフェース 60 を、衛星ネットワークに対して適切な周波数およびプロトコルへ合わせるよう動作し、かつ、(衛星ネットワークに対して適切な) 符復号器 59 b が選択される。故に、GSM ネットワークが選択されると、通信は、(図2に示される) 二重通信方式リンク 15 上で起こり、一方、衛星ネットワークが選択されると、通信は、衛星 3 a を介した二重通信方式リンク上で起こる。

【0044】図7を参照すると、料金前払 ICO 加入者によって生成された呼の経路決定が詳細に考察されている。該 ICO 加入者は、移動先の GSM ネットワーク内におり、使用者端末 UT 4 a を使用して、遠く離れた PSTN 6 内の送受器へ電話をかけている。料金前払加入

者は、料金前払 SIM 56 を有している。料金前払 SIM 56 は、例えば、契約番号に電話をかけることによって、かつ、希望する量のクレジットを購入するために (クレジットカードのような) 適切な支払手段を使用することによって、料金請求されることができる。フェーズ 2+ SIM ツールキット compliant SIM カード (Phase 2+ SIM Toolkit compliant SIMcard) のような料金前払 SIM 56 は、UT 4 a を制御するために、本発明に従ってセットアップされる。

【0045】概して言えば、料金前払 SIM 56 の機能は、クレジット照合確認メッセージを開始すること、許容呼期間を管理すること、UT 操作を制御することを含む。これらは、以下に、より詳細に説明される。

【0046】UT 4 a がスイッチを入れられると、UT 4 a は、該 UT 4 a のホームネットワークからサービスを得ることを試みる。もし、例えば、UT 4 a が (PLMN 8 のような) 他のネットワークのサービスエリアへ移動しているために、該サービスを得ることができないならば、第1ステップ (s1) は、UT 4 a が (それ自体がよく知られた方法で) PLMN 8 に関連する VLR 39 へ自己を登録することである。登録手続の結果として、SIM 56 は、移動先ネットワーク PLMN 8 の同一性を得る。

【0047】その後、加入者が (PLMN 8 を使用して) 電話をかけた場合、該加入者は、UT キーパッド 53 において、ターゲット電話 13 の番号を入力し、かつ、キーパッド上の 'SEND' ボタンを押す (s2)。SIM 56 は、UT 4 a が直ちに電話をかけることを禁止し、かつ、代わりに、使用者に適切なメッセージ (例えば、「クレジット照合中……お待ち下さい」) を表示することを、UT 4 a に指示する (s3)。そして、SIM 56 は、標準 GSM アンストラクチャードサブリメンタリサービスデータ (standard GSM Unstructured Supplementary Service Data: USSD) サービスを使用してメッセージをホームネットワークへ送信することを、UT に指示する。USSD サービスは、全ての GSM プロバイダによってサポートされている。USSD メッセージの内容は、移動先ネットワークの同一性 IMS I とダイヤル番号とを含む。該メッセージは、ホームネットワークによって決定された料金前払クレジット確認/保安プロトコルに従って、符号化される。

【0048】USSD メッセージは、ホームネットワーク MSC 21 によって受信される。ホームネットワーク MSC 21 は、メッセージを料金前払サーバー (PPS) 24 へ送る (s5) ように構成されている。PPS 24 は、各料金前払加入者に対するクレジット記録を含むデータベースを具備する。PPS は、例えば、専用コンピュータ上に実現される。

【0049】PPS 24 は、供給された IMS I 情報に基づいて加入者を識別し、かつ、該加入者に対応するク

レジット記録を検索する(ｓ6)。そして、PPS24は、移動先ネットワーク同一性とダイヤル番号情報と現在時刻情報とを使用して、該呼に適應する(PLMN8の)料金表を決定する(ｓ7)。該料金表情報は、ネットワークオペレータ間の標準移動契約に基づいて得られる。

【0050】利用可能なクレジットと適応可能な料金表とが分かると、PPSは、ネットワーク8上に生成されるべき特定の呼に対して許可される呼期間を計算する(ｓ8)。この情報は、ステップ9において、USSDメッセージ内で、MSSC21を介して、UTおよびSIMへ送信される。

【0051】SIMは、移動先ネットワーク8上での呼を可能にし、かつ、通常表示へ戻ることUTへ指示する(ｓ10)。該通常表示は、例えば、ダイヤルされている番号を表示する。そして、接続が確立すると、SIMは、内部タイマを起動する(ｓ11)。該内部タイマは、PPS24によって供給された時間からカウントダウンする。SIMは、この段階で可能な様々な表示を示すこと(例えば、残存している呼時間を表示すること)を、UTに指示してもよい(明確には示されていないステップ)。

【0052】タイマが呼の期間を終了すると、SIMは、呼を終了することを、UTに指示し(ｓ12)、かつ、(呼期間を示す)USSDメッセージをMSSC21へ返送することを、UTに指示する(ｓ14)。もし、タイマが終了する前に呼が終わるならば、SIMはタイマを停止し(ｓ13)、かつ、タイマ終了の場合と同様に、(呼期間を示す)USSDメッセージをMSSC21へ返送することを、UTに指示する(ｓ14)。いずれの場合にも、MSSC21は、USSDメッセージをPPS24へ送る(ｓ15)。PPS24は、残存呼時間を計算し、かつ、該残存時間を(加入者にクレジットされている)クレジット量に変換する(ｓ16)。SIM56は、料金前払クレジットを料金再請求するために、(ホームネットワーク番号への呼を除いては)更なる呼の試みを見合わせる。

【0053】他に、PPS24がSIMに利用可能な呼時間を知らせると、PPS24は、ステップ8において、クレジット記録をゼロに設定し、かつ、「期限満了になっていない時間が幾分残っている」ということを示すためにセットアップされるUSSDメッセージを受信する場合のみ、クレジット記録をリセットする。このこ

とは、もし、呼時間が終了するならば、UTがUSSDメッセージを返送する必要がある。

【0054】本発明は(加入者が該加入者のホームネットワーク以外のネットワークへ移動している間における)リアルタイムクレジット照合の点において説明されたが、「クレジット計算は、別のネットワーク上の別の料金表を考慮して、前もって実行されることができる」ということも見られる。そして、利用可能時間情報は、使用者端末が他のネットワークへ(引き続き)移動するときの使用のために、SIMカード内に記憶されることができる。

【0055】他に、呼のセットアップの度にクレジット照合を実行するよりもむしろ、クレジット照合は、1日毎にまたは他の周期に基づいて、実行されてもよい。例えば、例えば、UTがスイッチを入れられると、クレジット詳細がSIMカードに一時的に記憶される。そして、日中に生成された呼に対しては、SIMカードが、料金前払サーバーの代理を行い、一日の終わりにUTがスイッチを切られると、料金前払サーバーを更新するだけである。

【図面の簡単な説明】

【図1】 本発明による衛星遠距離通信システムの一例を示すブロック図である。

【図2】 衛星ネットワークおよび地上セルラーネットワークの一例を示すブロック図である。

【図3】 衛星ネットワーク内の料金前払サーバーの設備の一例を示すブロック図である。

【図4】 移動使用者端末の一例を示す概要図である。

【図5】 移動使用者端末の回路構成例を示すブロック図である。

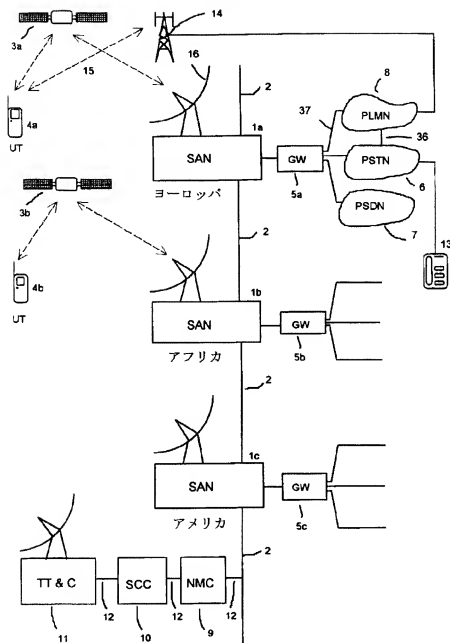
【図6】 SIMカードの一例を示すブロック図である。

【図7】 本発明によるクレジット照合手続の一例を示すフローチャートである。

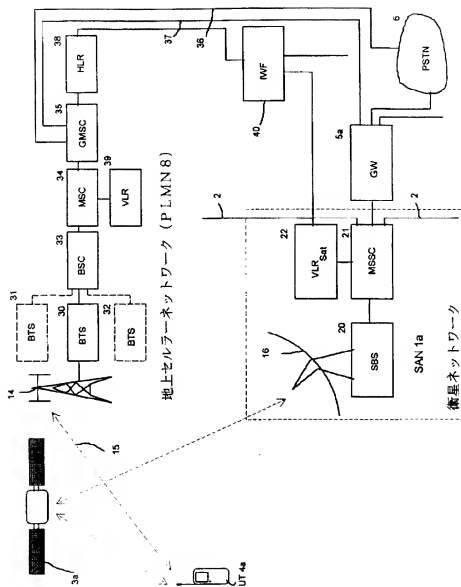
【符号の説明】

1a, 1b, 1c……衛星アクセスノード、2……バックボーンネットワーク、3a, 3b……衛星、4a, 4b……使用者端末、5a, 5b, 5c……ゲートウェイ、6……公衆交換電話ネットワーク、7……公衆交換データネットワーク、8……公衆地上移動ネットワーク、9……ネットワーク管理センター、10……衛星制御センター、11……追跡・遠隔測定・制御局

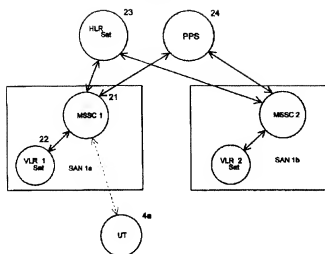
【図1】



地上セルラーネットワーク (PLMN8)

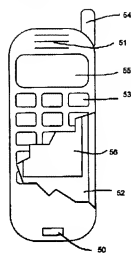


【図 3】

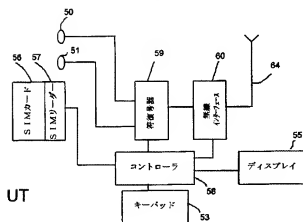


【図 4】

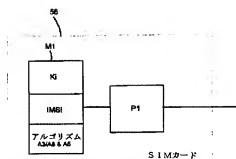
UT 4a



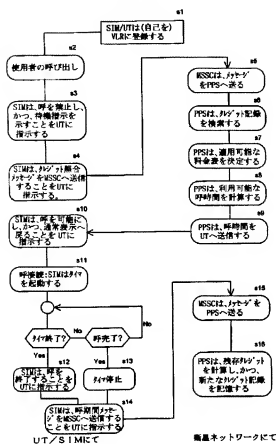
【図 5】



【図 6】



【図 7】



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-115353

(43)Date of publication of application : 21.04.2000

(51)Int.Cl.

H04M 1/675

G06F 3/08

H04B 7/26

H04M 1/725

H04M 11/00

(21)Application number : 10-276008

(71)Applicant : NTT MOBIL COMMUNICATION
NETWORK INC

(22)Date of filing : 29.09.1998

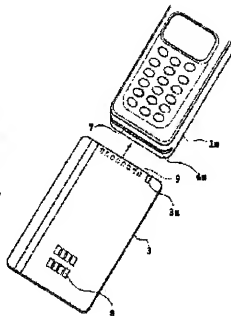
(72)Inventor : FURUSE MASAHIRO
HAMADA KATSUNORI
WAKABAYASHI TATSUAKI
ISHIKAWA HIDETOSHI

(54) MOBILE COMMUNICATION TERMINAL

(57)Abstract:

PROBLEM TO BE SOLVED: To easily read/write data or the like from/to an SIM mounted on a mobile communication terminal, without removing the SIM.

SOLUTION: Eight terminals of a connection section 4 of a main body 1a is connected electrically to 8 terminals of a card 3, by inserting (mounting) one end of the card 3 to a groove structure of the connection section 4 in a way such that a projection 4a of the main body 1a is inserted into a notch 3a of the card 3. Since a SIM 6 in a radio device 1 is connected electrically to a connection section 8 of the card 3, data are read from/written in the SIM 6 via the connection section 8 by inserting the card 3 to a reader/writer, while keeping this state (mounting the SIM 6 in the radio device 1).



(19)日本国特許庁(J P)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開2000-115353

(P2000-115353A)

(43)公開日 平成12年4月21日(2000.4.21)

(51)Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 M	1/675	H 0 4 M	1/66 E 5 B 0 6 5
G 0 6 F	3/08	G 0 6 F	3/08 C 5 K 0 2 7
H 0 4 B	7/26	H 0 4 M	1/72 B 5 K 0 6 7
H 0 4 M	1/725	11/00	3 0 2 5 K 1 0 1
	11/00	H 0 4 B	7/26 M
	3 0 2	審査請求	未請求 請求項の数5 O L (全 5 頁)

(21)出願番号 特願平10-276008

(22)出願日 平成10年9月29日(1998.9.29)

(71)出願人 392026893

エヌ・ティ・ティ移動通信網株式会社
東京都港区虎ノ門二丁目10番1号

(72)発明者 古瀬 正浩

東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内

(72)発明者 濱田 克雄

東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内

(74)代理人 100077481

弁理士 谷 義一 (外3名)

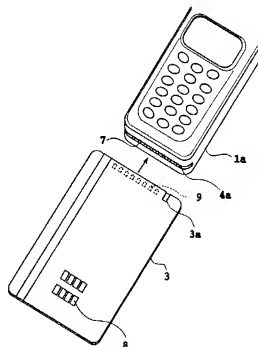
最終頁に続く

(54)【発明の名称】 移動通信端末

(57)【要約】

【課題】 移動通信端末に装着されたS I Mに対するデータ等の読み書きをS I Mを取り外すことなく容易に行うこと。

【解決手段】 カード3の切れ込み3 aに本体1 aの突起4 aが挿入されるようにして接続部4の溝構造にカード3の一端部を挿入(装着)することによって、本体1 aの接続部4の8個の端子とカード3の8個の端子とが電気的に接続される。これによって、無線機1内のS I M 6とカード3の接続部8とが電気的に接続されるので、この状態のまま(無線機1内にS I M 6を装着したまま)、カード3をリーダー・ライターに挿入することによって、接続部8を介して、S I M 6に対してリーダー・ライターからデータの読み書きを行うことができるようになる。



【特許請求の範囲】

【請求項 1】 所定の情報が記憶された記憶手段が装着される移動通信端末であって、ＩＣカードとほぼ同形状であって所定の位置に信号の入出力が可能な端子を持つカード状のカバーを有し、前記記憶手段と前記端子とが電気的に接続されることを特徴とする移動通信端末。

【請求項 2】 請求項 1 において、前記記憶手段はＳＩＭであることを特徴とする移動通信端末。

【請求項 3】 所定の情報が記憶された記憶手段が装着される移動通信端末であって、ＩＣカードとほぼ同形状であって所定の位置に信号の入出力が可能な端子を持つカード状のカバーを有し、前記記憶手段と前記端子とが電気的に接続されていることを特徴とする移動通信端末。

【請求項 4】 請求項 3 において、前記記憶手段はＳＩＭであることを特徴とする移動通信端末。

【請求項 5】 請求項 3 または 4 において、前記カバーは、折り畳み又はスライド可能であることを特徴とする移動通信端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、加入者情報等が記憶されたＩＣカード（以下、ＳＩＭ：Subscriber Identity Module）を搭載した移動通信端末に関する。

【0002】

【従来の技術】ＳＩＭはフルサイズのＩＣカードよりも小型であり、従来、加入者情報等が記憶されたＳＩＭが搭載された移動通信端末（携帯電話、ＰＨＳ等）が知られている。

【0003】

【発明が解決しようとする課題】上述のような移動通信端末においては、ＳＩＭはその通信端末内のソケットに装着されており、このＳＩＭ内の加入者情報あるいはこれに加えてアプリケーションを利用する際には、外部のリーダー・ライターにＳＩＭを接続しなければならない。そのためには、ＳＩＭを移動通信端末から取り外さなければならない。

【0004】さらに、小型なＳＩＭを移動通信端末から取り外すことは容易ではなく、取り外したＳＩＭを移動通信端末内のソケットに再び装着することも容易ではない。また、ＳＩＭの装着、取り外しは、ＳＩＭを移動通信端末内の所定のソケットに対して抜き差しすることによって行うが、このような抜き差しを行って、外部のリーダー・ライターと接続して読み書きを行うと、その接触部が著しく劣化してしまう。

【0005】そこで本発明の目的は、以上のような問題

を解消した移動通信端末を提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するため、請求項 1 の発明は、所定の情報が記憶された記憶手段が装着される移動通信端末であって、ＩＣカードとほぼ同形状であって所定の位置に信号の入出力が可能な端子を持つカード状の端子と接続するための接続部を有し、前記接続部を介して前記記憶手段と前記端子とが電気的に接続されることを特徴とする。

10 【0007】また請求項 2 の発明は、請求項 1 において、前記記憶手段はＳＩＭであることを特徴とする。

【0008】さらに請求項 3 の発明は、所定の情報が記憶された記憶手段が装着される移動通信端末であって、ＩＣカードとほぼ同形状であって所定の位置に信号の入出力が可能な端子を持つカード状のカバーを有し、前記記憶手段と前記端子とが電気的に接続されていることを特徴とする。

【0009】さらに請求項 4 の発明は、請求項 3 において、前記記憶手段はＳＩＭであることを特徴とする。

20 【0010】さらに請求項 5 の発明は、請求項 3 または 4 において、前記カバーは、折り畳み又はスライド可能であることを特徴とする。

【0011】

【発明の実施の形態】図 1 は本発明の第 1 の実施形態の正面図、図 2 は同背面図である。

【0012】1 は移動通信端末を構成する無線機であって、その本体 1 a の上部にはアンテナ 2 が設けられており、また、本体 1 a の下部には、後述するカード 3 と接続するための接続部 4 が設けられている。図 1、図 2 は本体 1 a の接続部 4 にカード 3 が装着された状態を示している。

【0013】本体 1 a の内部には、ソケット 5 が設けられており、このソケット 5 には加入者情報等が記憶されたＳＩＭ 6 が装着される（図 2 はソケット 5 に装着されていない状態のＳＩＭ 6 を示している）。

【0014】接続部 4 は、図 3 に示すようにカード 3 の一端部を緊密に挿入（装着）可能な溝構造を持つており、この溝の一方の内側に、カード 3 の 8 個の端子（後述）と電気的に接続するための 8 個の端子 7 が並設されている。この 8 個の端子 7 の各々はソケット 5 とリード線等で接続されている。

【0015】カード 3 は、フルサイズのＩＣカードと同一サイズを持ち、後述するような接続部および端子を有するものであって、その内部にＩＣ等の電子部品は有していない。このカード 3 の材質は例えばＩＣカードのそれと同一であっても良い。また、カード 3 は、ＩＣカードのそれと同一位置にＩＣカード用のリーダー・ライターに装着してデータを読み書きするための 8 個の接触部からなる接続部 8 が設けられている。さらにカード 3 の長さ方向の一端部には無線機 1 の本体 1 a の接続部 4 の 8 個

3

の端子と電気的に接続するための8個の端子9が並設されている。このカード3の一端部に設けられた8個の端子9の各々は接続部8の8個の接触部の各々とリード線等で接続されている。

【0016】なお、カード3の一方の側面の一端の1箇所には切れ込み3aが設けられており、これと対応するように、本体1aの接続部4の溝の他方の内側1箇所に突起4aが設けられている。

【0017】したがって、カード3の切れ込み3aに本体1aの突起4aが挿入されるようにして接続部4の溝構造にカード3の一端部を挿入（装着）することによって、本体1aの接続部4の8個の端子とカード3の8個の端子とが電気的に接続される（切れ込み3aに突起4aが挿入されるので、カード3の裏表を逆にして挿入されることはない）。これによって、無線機1内のSIM6とカード3の接続部8とが電気的に接続されるので、この状態のまま（無線機1内にSIM6を装着したまま）、カード3をリーダー・ライタに挿入することによって、接続部8を介して、SIM6に対してリーダー・ライタからデータの読み書きを行うことができるようになる。必要なデータ処理が終了したならば、カード3をリーダー・ライタから抜き出し、無線機1の本体1aからカード3を外すことによって、無線機1を使用することができる。

【0018】図4は本発明の第2の実施形態の正面図、図5は同背面図（詳細は後述するが、カバーを開じた状態、即ち折り畳まれた状態）である。

【0019】10は移動通信端末を構成する無線機であって、その本体10aの上部にはアンテナ11が設けられており、また、本体10aの下部には、本体10aのキーパッドを保護するカバー12の下端が回転可能に取り付けられている。本体10aの内部には、ソケット5が設けられており、このソケット5には加入者情報等が記憶されたSIM6が装着される。また、カバー12を閉じることによって、キーパッドは保護され、図4に示すようにカバー12を開くことによって、後述のように本体10a内のSIM6と、外部のリーダー・ライタとの間のデータのやり取りが可能となる。

【0020】カバー12は、フルサイズのICカードと同一サイズを持ち、その内部にIC等の電子部品は有していない。また、カバー12は、ICカードのそれと同

4

一位置にICカード用のリーダー・ライタに装着してデータを読み書きするための8個の接触部からなる接続部13が設けられている。ソケット5と接続部13の8個の接触部の各々とはリード線等で接続されている。これによって、無線機10内のSIM6とカバー12の接続部13とが電気的に接続されることになる。

【0021】したがって、カバー12を開いた状態で（無線機10内にSIM6を装着したまま）、カバー12をリーダー・ライタに挿入することによって、接続部13を介して、SIM6に対してリーダー・ライタからデータの読み書きを行うことができるようになる。

【0022】なお、カバー12は折り畳み式としたが、そのほかにスライド式とすることもできる。

【0023】

【発明の効果】以上説明したように本発明によれば、移動通信端末に装着された記憶手段（例えばSIM）に対するデータ等の読み書きを当該記憶手段を取り外すことなく容易に行うことができる。このため、例えば、前記記憶手段がSIMの場合は、サービス利用手順が容易になるという効果が得られる。また、記憶手段を取り外さなくても済むので、その接点等の劣化を防ぐことができる。さらに、移動通信端末の一部としてICカードと同形状のカバーを持つ場合は、信号の入出力を行う端子の劣化も防ぐことができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態の正面図である。

【図2】同背面図である。

【図3】同使用状態を示す斜視図である。

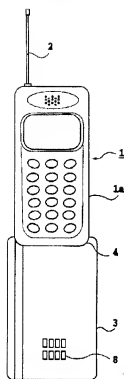
【図4】本発明の第2の実施形態の斜視図である。

【図5】同背面図である。

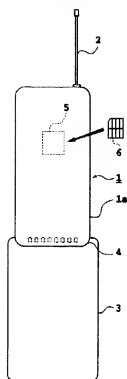
【符号の説明】

- 1 無線機
- 1a 本体
- 2 アンテナ
- 3 カード
- 4 接続部
- 5 ソケット
- 6 SIM
- 7, 9 端子
- 8 接続部

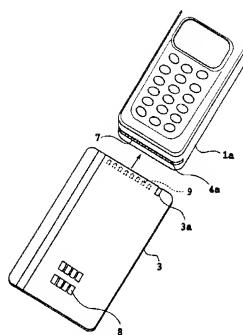
【図1】



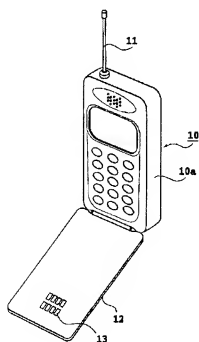
【図2】



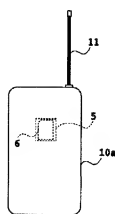
【図3】



【図4】



【図5】



フロントページの続き

(72)発明者	若林 達明	Fターム(参考)	5B065 BA09 ZA11
	東京都港区虎ノ門二丁目10番1号 エス・		5K027 AA11 BB02 BB09 HH23 KK07
	ティ・ティ移動通信網株式会社内		MM03
(72)発明者	石川 秀俊		5K067 AA34 BB04 BB21 DD51 EE03
	東京都港区虎ノ門二丁目10番1号 エス・		FF02 FF23 HH23 KK15 KK17
	ティ・ティ移動通信網株式会社内		5K101 KK20 NN40

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-279325

(43)Date of publication of application : 27.09.2002

(54)Int.Cl.

G06F 17/60

G06K 17/00

(21)Application number : 2001-076087

(71)Applicant : JR EAST MECHATRONICS CO LTD

(22)Date of filing : 16.03.2001

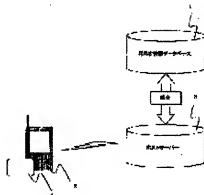
(72)Inventor : OGAWA KIYOTAKA
MORIYASU AKIYUKI
NANBU KEIICHI
SATO MASANOBU

(54) ELECTRONIC BUSINESS TRANSACTION SYSTEM USING CELLPHONE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a mobile electronic business transaction environment, used by a user at ease by taking security measures which are safer than the conventional one in a case of theft and loss in an electronic business transaction by a cellphone using SIM(subscriber identity module) card.

SOLUTION: This electronic business transaction system is provided with the cellphone 2 in which the SIM card 4 is inserted, a host server 3 on-line connected to the cellphone and having a function performing electronic business transaction, and users' information database 1 having a pre-registered combination of a cellphone number and SIM card identification information. When making transaction of the electronic business by on-line connecting to the cellphone, the host server collates the cellphone number and the SIM card identification information with the contents preregistered in the users database and, only when the collation result matches each other, will the value added information be downloaded to the cellphone.



(51) Int.Cl. ⁷	識別記号	F I	テロート [*] (参考)
G 0 6 F 17/60	4 1 4	G 0 6 F 17/60	4 1 4 5 B 0 5 8
	1 1 2		1 1 2 H
	1 4 6		1 4 6 A
	2 2 2		2 2 2
	3 3 0		3 3 0
審査請求 未請求 請求項の数 1 O L (全 3 頁) 最終頁に続く			

(21) 出願番号 特願2001-76087(P2001-76087)

(22) 出願日 平成13年3月16日 (2001.3.16)

(71) 出願人 593092482

ジェイアール東日本メカトロニクス株式会
社

東京都港区芝浦3丁目8番10号

(72) 発明者 小河清隆

東京都港区芝浦3丁目8番10号 ジェイア
ール東日本メカトロニクス株式会社内

(72) 発明者 森安亮之

東京都港区芝浦3丁目8番10号 ジェイア
ール東日本メカトロニクス株式会社内

(74) 代理人 100092495

弁理士 経川 昌信 (外7名)

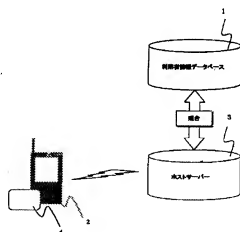
最終頁に続く

(54) 【発明の名称】 携帯電話を用いた電子商取引システム

(57) 【要約】

【課題】 SIMカードを用いた携帯電話による電子商取引において、盗難、紛失時にこれまで以上のセキュリティ対策を施し、利用者が安心して使用できるモバイル電子商取引環境を提供する。

【解決手段】 SIMカード(4)がセットされる携帯電話機(2)と、携帯電話機とオンライン接続して電子商取引を行う機能を有するホストサーバー(3)と、携帯電話番号およびSIMカード識別情報の組み合わせが事前登録された利用者情報データベース(1)とを備え、ホストサーバーは、携帯電話機とオンライン接続して電子商取引を行う際、携帯電話番号、SIMカード識別情報を利用者データベースに事前登録された内容と照合し、照合の結果一致する場合のみ付加価値情報を携帯電話機にダウンロードするようにしたものである。



【特許請求の範囲】

【請求項 1】 SIMカードがセットされる携帯電話機と、携帯電話機とオンライン接続して電子商取引を行う機能を有するホストサーバーと、携帯電話番号および SIMカード識別情報の組み合わせが事前登録された利用者情報データベースと、を備え、ホストサーバーは、携帯電話機とオンライン接続して電子商取引を行う際、携帯電話番号、SIMカード識別情報を利用者データベースに事前登録された内容と照合し、照合の結果一致する場合のみ付加価値情報を携帯電話機にダウンロードすることを特徴とする携帯電話による電子商取引システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は携帯電話を用いた電子商取引システムに関する。

【0002】

【従来の技術】 現在、携帯電話によりホストサーバーにオンライン接続し、付加価値情報をダウンロードする種々なサービスが提案されている。このようなモバイル EC（電子商取引）においては、盗難や紛失時のセキュリティ対策は、パスワードでの認証を行うのが一般的で、パスワードが一致しない場合にその携帯電話によるサービスを停止するというものである。

【0003】 ところで、携帯電話に SIM（加入者識別モジュール）カードをセットし、携帯電話として機能させる SIMカードシステムが提案され、欧州では既に普及し、日本においても近い将来、このシステムになると考えられている。SIMカードは機能的に ICカードと同等であり、1チップの ICにいろいろな個人情報（例えば、クレジットカード番号、定期券、チケット情報等）を格納している付加価値情報を格納することも提案されている。このような SIMカードを用いて携帯電話により電子商取引を行う際、カードの盗難や紛失時に対するセキュリティを確保することが必要である。

【0004】

【発明が解決しようとする課題】 しかしながら、従来の盗難、紛失時のセキュリティ対策は、パスワードでの認証が一般的で多くのパスワードは 4桁であり、生年月日等の個人情報を用いることが多く、解読される危険性が高い。本発明は SIMカードを用いた携帯電話による電子商取引において、盗難、紛失時にこれまでに以上のセキュリティ対策を施し、利用者が安心して使用できるモバイル電子商取引環境を提供しようとするものである。

【0005】

【課題を解決するための手段】 本発明の携帯電話による電子商取引システムは、SIMカードがセットされる携帯電話機と、携帯電話機とオンライン接続して電子商取引を行う機能を有するホストサーバーと、携帯電話番号および SIMカード識別情報の組み合わせが事前登録

された利用者情報データベースとを備え、ホストサーバーは、携帯電話機とオンライン接続して電子商取引を行う際、携帯電話番号、SIMカード識別情報を利用者データベースに事前登録された内容と照合し、照合の結果一致する場合のみ付加価値情報を携帯電話機にダウンロードすることを特徴とする。

【0006】

【発明の実施の形態】 以下、本発明の実施の形態を図面を参照しつつ説明する。図 1 は本発明の携帯電話による電子商取引システムを説明する概念図である。携帯電話機 2 には、SIM（加入者識別モジュール）カード 4 がセットされ、個人情報や電子商取引を行うための付加価値情報等の様々なデータが格納されている。ホストサーバー 3 は携帯電話機 2 とオンライン接続して電子商取引の処理を行い、取引が成立した時に携帯電話機に対して付加価値情報をダウンロードする機能を有している。利用者情報データベース 1 は電子商取引を行う携帯電話機 2 の電話番号と、そこにセットされる SIMカードの識別情報（例えば ID 番号）が事前に登録されている。

【0007】 電子商取引に際し、携帯電話機 2 からホストサーバー 3 へアクセスすると、SIMカード 4 の ID 番号が携帯電話番号とともにホストサーバー 3 へ通知される。ホストサーバー 3 は SIMカードの ID 番号と使用中の携帯電話番号の組み合わせについて利用者情報データベース 1 を参照して照合する。SIMカードの ID 番号と携帯電話番号の組み合わせが利用者情報データベース 1 に事前登録された内容と一致する場合のみ、ホストサーバー 3 は付加価値情報のダウンロード等のサービスを提供する。もし、不一致の場合は、サービス要求は受け付けず、これにより、SIMカードの盗難、紛失の場合に自分以外の携帯電話機からの利用ができなくなり、不正なモバイル電子商取引を防ぐことができる。

【0008】 本発明のシステムにおけるサービスは、例えば電子マネー、交通チケット、イベントチケットなどの付加価値情報を SIMカードにダウンロードして実際の店舗で使用する場合に適用可能である。

【0009】

【発明の効果】 以上のように、本発明によれば、携帯電話番号とカード識別情報とを事前に登録しておき、電子商取引に際しては、携帯電話番号とカード識別情報とを照合して事前登録した内容と一致する場合のみサービスを提供するようにしたので、カードの盗難や紛失時における不正なモバイル電子商取引を防ぐことができ、セキュリティを確保して電子商取引環境の向上を図ることが可能となる。

【図面の簡単な説明】

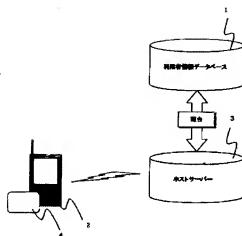
【図 1】 携帯電話による電子商取引システムを説明する概念図である。

【符号の説明】

1…利用者情報データベース、2…携帯電話機、3…ホ

ストサーバ、4…SIMカード。

【図1】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

テーマコード(参考)

G 0 6 F 17/60

5 0 6

G 0 6 F 17/60

5 0 6

5 1 0

5 1 0

G 0 6 K 17/00

Z E C

G 0 6 K 17/00

Z E C S

(72) 発明者 南部啓一

東京都港区芝浦3丁目8番10号 ジェイア
ール東日本メカトロニクス株式会社内

(72) 発明者 佐藤正信

東京都港区芝浦3丁目8番10号 ジェイア
ール東日本メカトロニクス株式会社内

Fターム(参考) 5B058 CA27 KA02 KA04 KA31 YA02

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-338814

(43)Date of publication of application : 28.11.2003

(51)Int.Cl.

H04L 9/32

G06F 15/00

G06K 17/00

G06K 19/10

H04Q 7/38

(21)Application number : 2002-145201

(71)Applicant : CANON INC

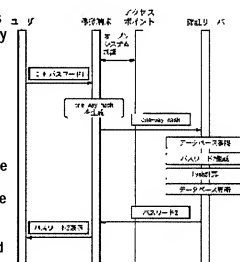
(22)Date of filing : 20.05.2002

(72)Inventor : KANDA TETSUO

(54) COMMUNICATION SYSTEM, ADMINISTRATIVE SERVER, CONTROL METHOD THEREFOR AND PROGRAM**(57)Abstract:**

PROBLEM TO BE SOLVED: To provide a high-security communication system in which a generated one-time password is surely delivered and illegal access from a third person is effectively blocked.

SOLUTION: In a management method for the communication system including a radio terminal on a wireless network and a server device for controlling access from the radio terminal to a wired network on the relevant wired network, an authentication procedure is implemented between the radio terminal and the server device and when first authentication information obtained from the radio terminal is authenticated by the server device in the authentication procedure, second authentication information in place of the first authentication information is generated. Then, the second authentication information is transmitted to the radio terminal while being contained in an authentication permission message as authentication information which can be authenticated by the radio terminal in the next authentication procedure.



(51) Int.Cl. ⁷	識別記号	F I	フォーマット [*] (参考)
H 0 4 L 9/32		G 0 6 F 15/00	3 3 0 C 5 B 0 3 5
G 0 6 F 15/00	3 3 0	G 0 6 K 17/00	T 5 B 0 5 8
G 0 6 K 17/00		H 0 4 L 9/00	6 7 3 D 5 B 0 8 5
19/10		G 0 6 K 19/00	R 5 J 1 0 4
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 S 5 K 0 6 7
		審査請求 未請求	請求項の数 9 ○ L (全 15 頁)

(21) 出願番号	特願2002-145201 (P2002-145201)	(71) 出願人	000001007 キヤノン株式会社 東京都大田区下丸子3丁目30番2号
(22) 出願日	平成14年5月20日 (2002. 5. 20)	(72) 発明者	神田 哲夫 東京都大田区下丸子3丁目30番2号 キヤ ノン株式会社内
		(74) 代理人	100076428 弁理士 大塚 康徳 (外3名)

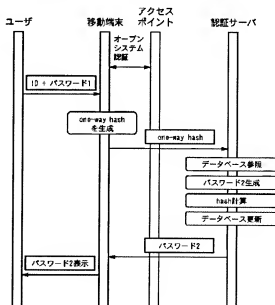
最終頁に続く

(54) 【発明の名称】 通信システム、管理サーバおよびその制御方法ならびにプログラム

(57) 【要約】

【課題】 生成したワンタイム・パスワードを確実に配送することができ、第三者からの不正アクセスを有効に防御できる安全性の高い通信システムを提供すること。

【解決手段】 無線ネットワークにおける無線端末と、有線ネットワークにおいて前記無線端末の当該有線ネットワークへのアクセスを制御するサーバ装置とを含む通信システムの管理方法であって、前記無線端末と前記サーバ装置との間で認証手順を実行し、その認証手順において、前記無線端末から得られた第1の認証情報が前記サーバ装置によって認証されたとき、第1の認証情報に変わる第2の認証情報を生成し、その第2の認証情報を前記無線端末が次の認証手順において認証可能な認証情報として認証許可メッセージに含めて前記無線端末に送信する。



【特許請求の範囲】

【請求項 1】 無線ネットワークにおける無線端末と、有線ネットワークにおいて前記無線端末の当該有線ネットワークへのアクセスを制御するサーバ装置とを含む通信システムであって、前記無線端末と前記サーバ装置との間で認証手順を実行する認証手段と、前記認証手順において前記無線端末より得られた第 1 の認証情報が前記サーバ装置によって認証されたとき、第 1 の認証情報にかわる第 2 の認証情報を、前記無線端末が次の認証手順において認証可能な認証情報として認証許可メッセージに含めて前記無線端末に送信する送信手段と、を備えることを特徴とする通信システム。

【請求項 2】 前記無線端末は、受信した前記認証許可メッセージに含まれる前記第 2 の認証情報を表示する表示手段を備えることを特徴とする請求項 1 に記載の通信システム。

【請求項 3】 前記無線端末は、メモ리카ードを装着するためのスロットと、前記第 1 の認証情報が記録されたメモ리카ードを前記スロットに装着することでその第 1 の認証情報を取得する取得手段と、受信した前記認証許可メッセージに含まれる前記第 2 の認証情報をもって前記メモ리카ードに記録されている前記第 1 の認証情報を書き換える書き換え手段と、を備えることを特徴とする請求項 1 に記載の通信システム。

【請求項 4】 本通信システムは、コネクションの確立手順を経ずに通信を行うコネクションレス型の通信システムであることを特徴とする請求項 1 から 3 までのいずれかに記載の通信システム。

【請求項 5】 無線ネットワークにおける無線端末と、有線ネットワークにおいて前記無線端末の当該有線ネットワークへのアクセスを制御するサーバ装置とを含む通信システムを管理する方法であって、前記無線端末と前記サーバ装置との間で認証手順を実行する認証ステップと、前記認証ステップで、前記無線端末から得られた第 1 の認証情報が前記サーバ装置によって認証されたとき、第 1 の認証情報にかわる第 2 の認証情報を、前記無線端末が次の認証手順において認証可能な認証情報として認証許可メッセージに含めて前記無線端末に送信する送信ステップと、を有することを特徴とする方法。

【請求項 6】 無線ネットワークおよび有線ネットワークを含む通信システムにおいて前記有線ネットワークにアクセスしようとする無線端末の当該アクセスを管理する管理サーバであって、前記有線ネットワークへの参加を許可する認証情報を登録した登録リストと、前記無線端末より受信した認証要求メッセージから得ら

れる第 1 の認証情報が前記登録リストに含まれているか否かによって認証を行う認証手段と、前記認証が成功したときに、前記無線端末の次の認証時に認証可能な認証情報としての第 2 の認証情報を生成する生成手段と、生成した前記第 2 の認証情報をもって前記登録リスト中の前記第 1 の認証情報を更新する更新手段と、生成した前記第 2 の認証情報を認証許可メッセージに含めて前記無線端末に送信する送信手段と、を備えることを特徴とする管理サーバ。

【請求項 7】 前記通信システムは、コネクションの確立手順を経ずに通信を行うコネクションレス型の通信システムであることを特徴とする請求項 6 に記載の管理サーバ。

【請求項 8】 無線ネットワークおよび有線ネットワークを含む通信システムにおいて前記有線ネットワークにアクセスしようとする無線端末の当該アクセスを管理する管理サーバの制御方法であって、前記有線ネットワークへの参加を許可する認証情報を登録した登録リストをあらかじめ記憶しておき、前記無線端末より受信した認証要求メッセージから得られる第 1 の認証情報が前記登録リストに含まれているか否かによって認証を行う認証ステップと、前記認証が成功したときに、前記無線端末の次の認証時に認証可能な認証情報としての第 2 の認証情報を生成する生成ステップと、生成した前記第 2 の認証情報をもって前記登録リスト中の前記第 1 の認証情報を更新する更新ステップと、生成した前記第 2 の認証情報を認証許可メッセージに含めて前記無線端末に送信する送信ステップと、を有することを特徴とする管理サーバの制御方法。

【請求項 9】 無線ネットワークおよび有線ネットワークを含む通信システムにおいて前記有線ネットワークにアクセスしようとする無線端末の当該アクセスを管理する管理サーバの制御プログラムであって、前記有線ネットワークへの参加を許可する認証情報をあらかじめ登録して記憶しておいた登録リストに、前記無線端末より受信した認証要求メッセージから得られる第 1 の認証情報が含まれているか否かによって認証を行う認証ステップ、前記認証が成功したときに、前記無線端末の次の認証時に認証可能な認証情報としての第 2 の認証情報を生成する生成ステップ、生成した前記第 2 の認証情報をもって前記登録リスト中の前記第 1 の認証情報を更新する更新ステップ、生成した前記第 2 の認証情報を認証許可メッセージに含めて前記無線端末に送信する送信ステップ、を実行させるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は通信システムに関し、特に、無線通信端末が無線ネットワークを介して有線ネットワークに参加するときの認証技術に関する。

【0002】

【従来の技術】無線LANシステムは従来より、通信ケーブルに拘束されない可搬性の優れたネットワークシステムとして利用されており、近年は特に、無線通信区間の伝送速度の向上や、ノート型パソコンの普及、モバイル通信に適したアプリケーションの出現などにより、飛躍的な普及を見せている。とりわけ2.4GHzや5GHz帯の電波を用いた無線LANシステムとして、IEEE802.11規格群によって規定された無線LANシステムが一般的に普及している。

【0003】しかしながら、このような無線LANシステムは高い利便性の反面、電波を用いたワイヤレス通信方式であるため、通信における秘密性や信頼性の低さが指摘されてきた。

【0004】たとえば、電波はその性質上、いったん送信機から空間中に出されると、宛先となるべき移動端末以外の第三者が傍受することが可能であり、情報としての通信データが外部の第三者に対して漏洩するおそれがある。また、無線LANシステムは、有線のLANがケーブルによって物理的に接続される運用形態ではなく、一般に移動端末の通信を管理する基地局に対しての無線通信手順によって論理的に接続される。したがって、自組織外の第三者の移動端末が過誤により、あるいは故意にネットワークに接続される事態が生じるおそれがある。

【0005】このような問題を防ぐために、無線LANシステムでは、上位のアプリケーション層から下位のMAC(Media Access Control)層、あるいは物理層までの各層において、各種の方法によって対策を行っている。とくに無線信号の傍受による情報の漏洩に対してはデータの暗号化などによって対応し、外部からの不正な接続に対しては認証方式を採用することによりこれらの問題を回避することが一般的である。具体的にはデータの暗号化方式としては、IEEE802.11規格によってWEP(Wire Equivalent Privacy)アルゴリズムを用いた共通秘密鍵方式が規定されており、一方、認証方式としては無線LANアクセスポイントの多くが、自組織に用いられる移動端末のMACアドレスを登録することによって、自組織外の第三者からのアクセスを防禦する方式がとられている。

【0006】さらに安全性を高めるべく、認証キーとして使用するパスワードを逐次変更していき、万が一パスワードが第三者に漏洩しても、新規に更新されたパスワードを用いることでそれ以降の不正アクセスを防ぐ方法が考えられている。かかる方法はいわゆるワンタイム・パスワード方式として知られている。このようなワンタイム・パスワード方式を携帯電話に適用した従来技術と

して特開平5-336109号が挙げられる。これによれば、電話での通話が終了する時に新たに乱数を発生し、この乱数を次の発呼時に認証キーとして利用する。つまり、新たな認証キーはコネクションの終了フェーズにおいて携帯電話に配送される。

【0007】

【発明が解決しようとする課題】しかしながら、このワンタイム・パスワード方式は、携帯電話のように接続と終話処理が明確であるコネクション型の通信システムには比較的適用しやすいものの、無線LANのようなコネクション型でない通信システムには適用が容易でないという問題がある。

【0008】具体的には、LANの運用形態では、例えばサーバへのアクセスの開始に際してセッションのログイン処理が行われるが、セッションの終了に際して必ずしも明確なログオフ処理を行うことは一般的に少なく、ユーザは端末利用が終わるとサーバへの接続開放などの手続きを行わず、端末の電源を切ってしまう場合が多い。さらに、LANは携帯電話のような通信システムよりもネットワークとしての接続性は低く、ネットワークの障害や、あるいは端末機器、サーバなどの停止によって、通信が強制的に終了してしまう事態も多く発生する。携帯電話システムがユーザの終話時に、セッションの終了フェーズとして通信チャネルの開放や課金情報の取り込みなど多くの処理を行うことに比べて、無線LANではセッションの終了が明確ではない。したがって、上記の携帯電話システムのようにコネクションの終了フェーズにおいて新たなパスワードを配送する方式のまま無線LANに適用する場合には、新たなパスワードを確実に配送することが保証されないことになる。

【0009】そこで、本発明は、生成したワンタイム・パスワードを確実に配送することができ、第三者からの不正アクセスを有効に防御できる安全性の高い通信システムを提供することを目的とする。

【0010】

【課題を解決するための手段】本発明の第1の側面は、無線ネットワークにおける無線端末と、有線ネットワークにおいて前記無線端末の当該有線ネットワークへのアクセスを制御するサーバ装置とを含む通信システムおよびその管理方法に関する。この第1の側面によれば、本通信システムは、前記無線端末と前記サーバ装置との間で認証手順を実行し、前記認証手順において前記無線端末より得られた第1の認証情報と前記サーバ装置によって認証されたとき、第1の認証情報にかかる第2の認証情報を、前記無線端末が次の認証手順において認証可能な認証情報として認証許可メッセージに含めて前記無線端末に送信する。

【0011】本発明の第2の側面は、無線ネットワークおよび有線ネットワークを含む通信システムにおいて前記有線ネットワークにアクセスしようとする無線端末の

当該アクセスを管理する管理サーバおよびその制御方法に関する。この第2の側面によれば、前記管理サーバは、前記有線ネットワークへの参加を許可する認証情報を登録した登録リストを有しており、前記無線端末より受信した認証要求メッセージから得られる第1の認証情報が前記登録リストに含まれているか否かによって認証を行い、前記認証が成功したときに、前記無線端末の次の認証時に認証可能な認証情報としての第2の認証情報を生成し、生成した前記第2の認証情報をもって前記登録リスト中の前記第1の認証情報を更新し、そして、生成した前記第2の認証情報を認証許可メッセージを含めて前記無線端末に送信する。また、この制御方法による一連の処理は、プログラムによっても実現される。

【0012】

【発明の実施の形態】本発明の利点を説明する前に、認証技術に関する予備的事項を追加的に説明しておく。

【0013】まず、IEEE802.11規格によって規定されたWE Pアルゴリズムを用いた共通鍵認証方式について説明する。

【0014】図6は一般的な無線LANシステムの構成を示した図である。無線LANステーション（STA）21は、図示のように移動端末211に無線LANカード212が装着された構成である。IEEE802.11規格では、アクセス方式としてアドホックモード、およびインフラストラクチャモードの2種類が定義されており、通常一時的な無線通信、例えばSTAとSTAの対一通信のような簡単なトポロジー構成ではアドホックモードが用いられ、一方、多数の移動端末がアクセスする大きなネットワーク構成ではインフラストラクチャモードが用いられる。インフラストラクチャモードでは、基地局として図中に示したアクセスポイント（AP）22が移動端末の制御をつかさどる。さらに、アクセスポイントは有線ネットワーク23に接続され、移動端末との無線区間での通信と有線基幹ネットワークでの通信の橋渡しをする。

【0015】IEEE802.11による認証方式としては、鍵を用いないオープンシステム認証方式と、STAが同一の共通秘密鍵を持つ共通鍵認証方式の2種類が規定されている。このうち図7はWE Pアルゴリズムによる共通鍵認証方式による動作を示したシーケンス図である。この認証処理は、例えば2個のSTAのみから構成されるアドホックモードにおいてはSTA間で、アクセスポイントを介したインフラストラクチャモードにおいては、STAからアクセスポイントへの認証動作となる。本図はインフラストラクチャモードにおけるSTAからAPへの認証動作を表している。

【0016】まず、本図において認証要求を求める移動端末（STA）はアクセスポイントに対して認証要求のための第1のマネジメントパケット（P1）を送出す

る。このP1は移動端末に装着された無線LANカードのMACアドレスを保持し、平文で伝送される。アクセスポイントはP1を受け取る、とアクセスポイントに具備された乱数発生器によりランダムな128ビットのデータを生成し、このランダムデータを第2のマネジメントパケット（P2）として、認証要求を行ったSTAに対して返送する。ここで、このS2はチャレンジテキストと呼ばれる。

【0017】次に、このチャレンジテキストを受信した移動端末はWE Pを起動する。図8はWE Pアルゴリズムによる暗号化ブロックの構成図である。ここで、WE Pアルゴリズムで使用される暗号化キーは、共通鍵部分（Shared Key）とイニシャライゼーション・ペクタ（IV）から構成される。共通鍵は一般にESSIDと呼ばれ、あらかじめ管理者によってすべての移動端末とアクセスポイントに同一の鍵が設定されている。一方、イニシャライゼーション・ペクタは暗号化を行うSTAが任意に生成するキーであり、パケット伝送ごとにパケットに添付されて相手先に伝えられる。

【0018】ここで、暗号化を行う移動端末はイニシャライゼーション・ペクタとして24ビットの任意の値を決定する。移動端末はこのイニシャライゼーション・ペクタと40ビットの共通秘密鍵を連結した64ビット値を乱数発生器に乱数シードとして与える。乱数発生器はこの乱数シードから暗号キーストリームとしての乱数系列（Key Sequence）を生成し、伝送される平文データ（Plain Text）とこの乱数系列との排他的論理和演算によって暗号化テキスト（Cipher Text）が生成される。また同時にデータの完全性を確認するために、CRC-32によるインテグリティ・アルゴリズムによって、一種のチェックサムとして32ビットのICVが生成される。このようにして作られた暗号化テキスト、IV、ICVはすべてパケット伝送によって相手先に伝えられる。

【0019】このWE Pアルゴリズムはデータパケットの暗号化に使用されるが、いま説明している認証シーケンスにおいては、STAはこのWE Pアルゴリズムにより、APから受け取ったチャレンジ・テキストを暗号化する。図7のシーケンス図において、STAは受信したチャレンジテキスト（P2）に対して、これを暗号化したデータパケット（P3）をアクセスポイントに対して送信する。ここで、S3はWE Pアルゴリズムによって生成された暗号化パケットであり、暗号化テキストと共に暗号化に用いられたIV、さらにデータ整合性の確認のためのICVが添付されてAPに伝えられる。

【0020】アクセスポイントは内部に実装されたWE P復号化ブロックによってこのP3パケットの検査と解読を行う。アクセスポイントでは図9に示すWE P復号化ブロックにて、あらかじめ設定された40ビットの共通秘密鍵、および受信した暗号化P3に含まれるIVから、暗号化ブロックと同様に64ビットの乱数シードを生成

し、この乱数シードから乱数発生器が乱数系列を生成する。共通秘密鍵、およびIVはSTAで暗号化された時に使われたものと同一であるので、ここで作られる乱数系列はSTAで暗号化されたときの系列と同じになり、結果としてアクセスポイントはSTAによって暗号化されたチャレンジテキストを解読することができる。

【0021】アクセスポイントは復号した平文から、マゼンテグリティ・アルゴリズム検査部で受信した平文のICVを計算し、受信パケットに記録されているICVとの比較を行う。これが同一であれば、次に復号化した平文がP2において自分からSTAに対して送出したチャレンジテキストと同一であるかを比較する。この結果、チャレンジテキストが同じであれば、アクセスポイントは当該STAが同一の共通鍵を持つ相手だと認識し、認証が成功する。アクセスポイントはこの認証結果を第4のマネジメントパケット(P4)によってSTAに通知し、認証処理が完了する。

【0022】以上、述べてきたのはIEEE802.11規格によって規定されている無線LANの認証方式である。しかしながら、このようなWE Pアルゴリズムによる認証方式だけでは、無線ネットワークの十分な安全性は確保できないと考えられる。なぜなら、WE Pアルゴリズムではアクセスポイント、および移動端末が共通に保持する共通鍵を確認することで認証を行っているだけであり、この鍵を知りえた外部の第三者は、自分の移動端末にこの共通鍵を設定することで容易に当該無線ネットワークへアクセスすることが可能となるからである。特に、この共通鍵の設定は例えばコンピュータシステム上で利用者が手入力で行うことができるため、利用者にとって比較的容易な手段で不正アクセスすることが可能である。さらに、多数の移動端末が同一の共通鍵を使用するようなシステムでは、共通鍵が外部に知られてしまう危険性は大きく、意図的な悪意の第三者による不正アクセスに対しては十分に安全な防衛方法とはならないといえる。

【0023】そのため一般の無線LANシステムでは、IEEE802.11規格によるWE Pアルゴリズム認証以外にも、MACアドレス登録機能を利用した認証方式を併用している。これは、あらかじめすべての移動端末に装着された無線LANカードの持つ6バイトのMACアドレスを、アクセスポイントに実装されたMACアドレス管理データベースに登録する方法である。無線区間を伝送するすべてのマネジメントフレーム、データフレームには、そのパケットを送出した発信元のMACアドレスが記録されているため、アクセスポイントはそのMACアドレスを確認することによって自組織内の正当な移動端末からのアクセスであるかどうか判断することができる。例えば図7に示した認証シーケンスにおいて、第1のマネジメントパケット(P1)には認証要求をしている移動端末のMACアドレスが記録されている。したが

って、アクセスポイントは本認証要求パケットのMACアドレスが、自分の持つMAC管理用データベースに登録されているかどうかの検索を行い、もしも未登録のアドレスであれば認証シーケンスの過程で認証処理を不成功にすることができる。

【0024】このようなMACアドレス登録方式の利点は、MACアドレスが無線LANカードの製造時にそれぞれのカードにユニークに実装されるアドレスであり、仮に第三者が無線ネットワーク上のアクセスポイントに登録されているMACアドレスのひとつを知りえたとしても、MACアドレスの書き換えには無線LANカードに実装されている不揮発性メモリなどの該当するアドレスの内容を書き換えるような操作が必要であり、前述のWE P共通鍵の設定と比較すると困難な作業となる。また、自分がなりすましたMACアドレスを持つ正当な無線LANカードが同時に稼働している場合には、マネジメントフレーム、データフレームの流れの不一致性などから、アクセスポイントによって不正アクセスを検出されやすく、WE Pアルゴリズムのみの認証方式と比較すると、より安全性の高いシステムといえる。

【0025】しかしながら、このようなアクセスポイントによるMACアドレスを管理する方法の欠点としては、当該無線ネットワークに参加すべき移動端末すべてのMACアドレスをアクセスポイントに登録しなければならない点が挙げられる。特にアクセスポイントが複数個存在する場合には、すべてのアクセスポイントに対して、このMACアドレス登録の作業が必要となり、ネットワーク管理のための工数が飛躍的に増大する。仮にアクセスポイントが数十台、数百台もあるような大規模な組織であれば、すべてのアクセスポイントへのMACアドレス登録を正しく保守、管理する作業は現実的と言えない。

【0026】したがって大規模なネットワークにおいてMACアドレスによる認証方式を利用するためには、MACアドレスをアクセスポイントに登録するのではなく、アクセスポイントの他に認証処理を制御する単一のサーバを準備し、この認証サーバのみにMACアドレスを登録することによって少ない工数でネットワーク全体の安全性を管理できるようにする技術もある。このような従来技術としては、例えば特開2001-111544号に記載されているようなものがあげられる。図10はこの従来技術による無線LANシステムの構成を示した図である。図中、有線ネットワーク23には認証サーバ25が接続されていることが特徴である。この従来例では認証方式としてRADIUS (Remote Authentication Dial In User Service) 方式を利用しており、認証サーバはRADIUSサーバによって移動端末のMACアドレスを登録された管理用データベースを具備している。一方、アクセスポイントにはMACアドレスのデータベースを持っておらず、RADIUSクライアントとして動作する。

【0027】図11は一般的な認証処理を示したシーケンス図である。まず、無線ネットワークに参加しようとする移動端末は、アクセスポイントに対して認証要求を送出する。この認証要求パケットには当該移動端末のMACアドレスが記録されている。要求を受けたアクセスポイントは、通常のWEPアルゴリズムではチャレンジテキストを移動端末に返送するが、ここではアクセスポイントから認証サーバに対して、移動端末のMACアドレスを認証のIDとして送出する。ここで、認証サーバはRADIUSプロトコルによってアクセスポイントから受け取った移動端末のMACアドレスを認証する。次に認証に成功した認証サーバは、アクセスポイントに対してチャレンジテキストを送出する。認証サーバからチャレンジテキストを受け取ったアクセスポイントは本来のWEPアルゴリズムに戻って、移動端末に対するチャレンジテキストを移動端末へ送信する。

【0028】以後、通常のWEPアルゴリズムにしたがって、移動端末はアクセスポイントから受信したチャレンジテキストに対し、共通鍵とIVにより暗号化を行う。この暗号文とIVは移動端末からアクセスポイントへ送信され、アクセスポイントはこの暗号文を解読し、ICVなどのチェックを経て認証を行う。そして、認証に成功したアクセスポイントは認証サーバにレスポンスを返す。

【0029】上述の図11に示したようなネットワーク構成では、認証処理に利用するMACアドレスのデータベースは認証サーバによって一元的に管理されているため、管理者はこのデータベースのみを更新することによって当該ネットワークに含まれる移動端末のMACアドレスを完全に管理することができるようになり、すべてのアクセスポイントにMACアドレスを登録する場合と比較し簡便にネットワークを管理することが可能となる。このようにして、IEEE802.11規格に規定されたWEPアルゴリズムに、さらに認証サーバによる移動端末のMACアドレス管理方式を追加することによって、より高度な認証を行っている。

【0030】上記のとおり、MACアドレスによる認証方式を追加することで、IEEE802.11規格に規定されたWEPアルゴリズムのみの認証方式よりも安全性が高められ、またMACアドレスの管理を認証サーバで一元的に行うことで保守作業の簡易化も図れることがわかる。

【0031】しかしながら、これまで説明してきた各方式では、認証のキーとして用いているWEP共通鍵やMACアドレスなどの情報は、すべて機器としての無線LANカード、あるいはそれが装着されている移動端末に割り振られているものであり、実際の使用者に対しての認証が行われているわけではない。これらの認証処理は、正当な機器は正当な利用者によって利用されているという前提によってなされているものであり、例えば紛失や盗難によって無線LANカード自体を手入した外部の第三者にとっては、本認証システムにおいてネット

ワークにアクセスすることは可能である。あるいは、非常に巨大な組織では、ある移動端末は複数の利用者によって使用されたり、逆に一人の利用者が複数の移動端末を利用することも多く、このような流動的な組織では頻繁に新たな無線端末が導入されたり、廃棄されたりなどするため、MACアドレスによる機器レベルの管理では、不具合が生じることも多い。

【0032】さらに、「なりすまし」のために自らの移動端末のMACアドレスを書き換える作業をいとわない悪意の第三者に対しては、MACアドレス管理による認証方式でさえ十分な認証方法とは言えない。当該ネットワークに参加を許された移動端末のMACアドレスを知り得た悪意の第三者は、自分の移動端末から当該MACアドレスを用いることにより、正当な端末にすり替えることが可能である。この場合、さらに悪いことにMACアドレスはそれぞれの移動端末に装着された無線LANモジュールに製造時に割り振られた数字であり、利用者はこれを自由に変更することはできないため、いったん自組織のMACアドレスが外部に漏れた場合には、正当な利用者はこのMACアドレスを持った無線LANカードを使い続けることができなくなる。このような事態は、認証方式に用いるキーとして、永久に固定値となるMACアドレスのようなデータを用いていることに起因する。すなわち、通信ネットワークにおいて、十分に安全で管理の容易な認証方式として使用する認証キーとしては、すべての移動端末とアクセスポイントが共通の鍵を持つ方式よりも、移動端末あるいは利用者が個々に設定できる認証キーが有効であり、さらに万が一、その認証キーが外部に漏れた際には、遅滞なく新しい認証キーに変更できるような柔軟な方式が望ましいといえる。

【0033】また、これまで挙げてきた例による認証方式では、ネットワークを利用するユーザーに対して認証を行っているだけでなく、ESSIDを登録された移動端末、あるいはMACアドレスを持った無線LANカードなど、通信機器に対しての認証を行う方式であった。ネットワークに対して実際に不正アクセスを試みるのは利用者であり、無線LANシステムのみならず一般に通信ネットワークにおいて高度な安全性を必要とする場合、MACアドレス管理のような機器に対する認証方式ではなく、利用者個人を正当なユーザーであるか外部の第三者であるかを特定できるような認証方式が必要となる。

【0034】図12は、利用者認証するシステムの例として、RADIUS認証サーバを用いてユーザーレベルでの認証システムを構築したネットワーク構成を示す例である。この例において、認証サーバ25に登録されている認証キーは無線LANカードのMACアドレスではなく、利用者31のa～cそれぞれのユーザーIDと個々のパスワードである。ユーザーIDは複数の利用者を識別するために用いられる個々にユニークな文字列であり、これらの値は組織内部、あるいは組織外部に対して公開

されていても何ら問題はない。一方、パスワードについては、一般にユーザ31-a~cはそれぞれ自分しか知らない文字列を決定し、あらかじめ認証サーバに登録しておく。

【0035】図13は本システムにおけるユーザ認証の手順を示したシーケンス図である。すべての利用者31はそれぞれ固有のユーザIDを持ち、それぞれ自分しか知らないパスワードを持つ。そして認証サーバに具備された認証用データベースには、これらユーザIDとパスワードがすべてあらかじめ登録されているものとする。

【0036】図13において、ネットワークにアクセスしたいユーザは、移動端末に自分のユーザIDとパスワードを入力する。移動端末とアクセスポイントはIEEE802.11規格に定められたオープンシステム認証によって認証が済んでおり、移動端末はアクセスポイントに対して下層でのアクセスは可能である。ここで、移動端末はRADIUSクライアントとして、ユーザから入力されたIDとパスワードから、一方方向ハッシュ(one-way hash)操作によりハッシュデータを生成する。移動端末はこのハッシュをアクセスポイントに対して送出し、アクセスポイントはこれを有線ネットワークを介して認証サーバに伝える。認証サーバはRADIUSサーバとして働き、自分の持つ認証用データベースに登録されているすべてのユーザIDおよびパスワードから、移動端末と同じ一方方向ハッシュ操作によりハッシュデータを生成しておき、移動端末から受信したハッシュと、データベース上のハッシュを比較する。この検索操作でデータベース上に当該ハッシュが存在すれば、受信したハッシュがあらかじめ登録されている正当な利用者からのものであることが識別できるため、認証が成功する。認証サーバはこの認証結果をアクセスポイントを通じて移動端末に伝え、その結果を表示された利用者は自分がネットワークにアクセスできることを知る。

【0037】以上説明したような、単一の認証サーバによるユーザレベルでのIDとパスワードを管理する方式は、従来の無線LAN認証方式としては非常に高度な安全性を持った方式といえる。

【0038】そして、さらに安全性を高めるために、いわゆるワンタイム・パスワードを使用することが考えられる。携帯電話システムでは、コネクションの終了フェーズにおいてワンタイム・パスワードを配送することが便宜であると考えられる。しかし、従来の技術の項で述べたとおり、コネクションの終了フェーズにおいてワンタイム・パスワードを配送することを、セッションの終了が明確でないことが多量無線LANのようなコネクションレス型の通信システムに適用すれば、ワンタイム・パスワードの確実な配送が保証され得ないことは明らかである。

【0039】そこで、本件発明者は、生成したワンタイム

ム・パスワードをセッション終了時に配送するのではなく、認証許可メッセージに含めて配送することを提案する。

【0040】以下、本発明の好適な実施形態について詳細に説明する。

【0041】実施形態における無線LANシステムのネットワーク構成は図12に示したとおりのものであり、無線端末としての移動端末13と、有線ネットワーク23に接続されたアクセスポイント(基地局)22および認証サーバ25とを含んでいる。移動端末13とアクセスポイント22とで無線ネットワークが構成され、このアクセスポイント22が無線ネットワークと有線ネットワーク23との中継を行う。また、この無線LANシステムは、コネクションの確立手順を省略して通信を行うコネクションレス型の通信システムである。

【0042】図2は認証サーバ25の内部構成例を示す図である。認証サーバ25は、有線LANトランシーバ2によって有線ネットワーク23に接続され、アクセスポイント22を介して移動端末13との通信を行う。さらに、認証サーバ25は認証用データベース121を記憶している。認証用データベース121には、ユーザ認証のための各ユーザ(31-a~c)のユーザIDと、それぞれのユーザに対して現在設定されているパスワード、およびこれらユーザIDとパスワードから計算された一方方向ハッシュが登録されている。また、認証サーバ25には入力手段としてのキーボード132と表示手段としてのディスプレイ122が設けられており、管理者はこれらを用いて認証データベース121の管理を行うことができる。

【0043】図3は移動端末13の構成例を示した図である。移動端末13は無線LANモジュール5を具備し、これに装着されたアンテナ14によってアクセスポイント22と無線通信を行い、アクセスポイント22を介して認証サーバ25と通信する。さらに、移動端末13は入力手段としてのキーボード132および表示手段としてのディスプレイ131を具備する。

【0044】図1は、実施形態における無線LANシステムでの認証処理を示すシーケンス図である。移動端末13を用いて有線ネットワーク23に参加しようとするユーザは、まず移動端末13のキーボード132から自分のユーザIDおよびパスワードを入力する。図1のシーケンス図に示したように、移動端末13は入力されたユーザIDとパスワードから一方方向ハッシュを生成する。ここで現在設定されているパスワードをパスワード1とする。あらかじめオープンシステム認証によってアクセスポイント22に対して認証が取れている移動端末13は、アクセスポイント22へこの一方方向ハッシュを接続要求パケットとして無線伝送する。本実施形態においてはアクセスポイント22自体は認証機能を持っておらず、アクセスポイント22は移動端末13から受け取

った一方ハッシュをそのまま有線ネットワーク 23 を介して認証サーバ 25 に中継する。

【0045】移動端末 13 からこの一方ハッシュを受け取った認証サーバ 25 は、自分の持つ認証用データベース 121 の登録内容を検索する。この結果、受け取ったハッシュと同一のハッシュが存在する場合、この認証要求は正当なユーザからのものであると判断し、認証が成功する。

【0046】その後、認証サーバ 25 は、このユーザ向けのワнтаム・パスワードとして新規パスワード（パスワード 2）を生成する。認証サーバ 25 はこのユーザ ID と新たに生成したパスワード 2 を用いて一方ハッシュを計算し、新規パスワードおよび新規ハッシュをもって認証用データベース 121 の当該ユーザ欄を更新する。そして、認証サーバ 25 はこのパスワード 2 を認証許可メッセージである認証許可パケットに含めてアクセスポイント 22 経由で移動端末 13 に返送する。認証許可パケットを受け取った移動端末 13 は図 3 に示したディスプレイ 131 にこのパスワード 2 を表示しユーザに伝える。ユーザは、表示されたパスワード 2 を記憶しておき、次回ログイン時にこのパスワード 2 を用いてログインすることができ。

【0047】このように、上述の実施形態によれば、生成されたワнтаム・パスワードはセッション終了時に配送されるのではなく、認証許可メッセージに含められて配送される。したがって、特に、コネクションの確立手順を経ずに通信を行うコネクションレス型でセッションの終了が明確でない通信システムにおいても、ワнтаム・パスワードを確実に配送することができる。

【0048】なお、上述した例の移動端末 13 は、受け取ったワнтаム・パスワードをディスプレイ 131 に表示してユーザに通知する構成であったが、移動端末 13 に内蔵されたメモリまたは読取自在のメモリ等へ書き込むようにしてもよい。以下、具体例を示す。

【0049】図 4 は他の実施形態における移動端末 13 の構成を示した図である。本図において、移動端末 13 はカードスロット 133 を具備する。カードスロット 133 は、フラッシュメモリ等のチップを内蔵したいわゆるメモリカード（スマートカードとも称される）15 を着脱できる構造となっており、さらにメモリカード 15 はこの移動端末 13 によってその内容が書き換えられるものとする。このメモリカード 15 は有線ネットワーク 23 への参加を許可されているユーザに対してあらかじめ配布されており、その記録内容として、それぞれのユーザのユーザ ID および初期パスワードが記録されている。

【0050】図 5 は、図 4 の構成を有する移動端末 13 に対する認証処理の一例を示すシーケンス図である。まず、移動端末 13 を用いてネットワーク 23 に参加しようとするユーザは、カードスロット 133 にユーザのメモ

リカード 15 を装着する。移動端末 13 は、このメモリカード 15 が装着されたことを検出すると、メモリカード 15 に記録されているユーザ ID および初期パスワード（パスワード 1）を読み込む。そして移動端末 13 は、これらユーザ ID およびパスワード 1 から一方ハッシュを生成し、これをアクセスポイント 22 へ接続要求パケットとして無線伝送する。そして、アクセスポイント 22 は移動端末 13 から受け取った一方ハッシュを有線ネットワーク 23 を介して認証サーバ 25 に中継する。

【0051】移動端末 13 からこの一方ハッシュを受け取った認証サーバ 25 は、認証用データベース 121 の登録内容を検索する。この結果、受け取ったハッシュと同一のハッシュが存在した場合、この認証要求は正当なユーザからのものであると判断し、認証が成功する。その後、認証サーバ 25 はこのユーザ向けの新規パスワード（パスワード 2）を生成する。認証サーバ 25 はこのユーザ ID と新たに生成したパスワード 2 を用いて一方ハッシュを計算し、新規パスワードおよび新規ハッシュをもって認証用データベース 121 の当該ユーザ欄を更新する。そして、認証サーバ 25 はこのパスワード 2 を含んだ認証許可パケットをアクセスポイント 22 経由で移動端末 13 に返送する。認証許可パケットを受け取った移動端末 13 は、この認証許可パケットからパスワード 2 を読み取り、メモリカード 15 に記録されたパスワード 1 をパスワード 2 に書き換える。このとき、同時にディスプレイ 131 に接続が許可された表示される。

【0052】ユーザは移動端末 13 の使用が終了した時には、このメモリカードを移動端末 13 から抜き取り、これを管理することになる。このように、メモリカードによってパスワードを管理することにより、ユーザが毎回更新されるパスワード（ワнтаム・パスワード）をその都度記憶しておく必要がなくなるという利点がある。

【0053】以上説明したように、本発明の実施形態によれば、無線 LAN システムにおいてワнтаム・パスワードを用いることにより、パスワードの盗難による第三者からの不正アクセスを防止することができる。ここで、パスワードの更新がログイン直後に行われるので、無線 LAN のようなコネクションレス型の無線ネットワークのようにセッションの終了が明確でない運用形態においても、生成されたワнтаム・パスワードが確実に配送され、次回ログイン時に正しく接続することができる。

【0054】このワнтаム・パスワードを用いた認証手順によれば、方が一、第三者による不正アクセスがあった場合、この第三者からの接続時に認証サーバでパスワードの更新が行われるため、正当なユーザによる次回ログイン時に、ユーザと認証サーバ間のパスワードが

致しないため、それ以前に不正アクセスがあったことを検知することもできる。このように、無線LANシステムに本発明を適用すれば、従来よりも不正アクセスに対する安全性を高めることができるようになる。

【0055】なお、上述の実施形態では認証プロトコルとしてRADUSサーバシステムを例に用いたが、一般的にユーザ認証方式として利用できる他の認証プロトコルを用いることも可能である。

【0056】

【他の実施形態】以上、本発明の実施形態を詳述したが、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リダー、プリンタ等）から構成されるシステムに適用しても、1つの機器からなる装置（例えば、複写機、ファクシミリ装置等）に適用してもよい。

【0057】なお、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムを、システムあるいは装置に直接あるいは遠隔から供給し、そのシステムあるいは装置のコンピュータがその供給されたプログラムを読み出して実行することによって達成される場合を含む。

【0058】したがって、本発明の機能処理をコンピュータで実現するために、そのコンピュータにインストールされるプログラムコード自体も本発明を実現するものである。つまり、本発明の特許請求の範囲には、本発明の機能処理を実現するためのコンピュータプログラム自体も含まれる。

【0059】その場合、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、OSに供給するスクリプトデータ等、プログラムの形態を問わない。

【0060】プログラムを供給するための記憶媒体としては、例えば、フレキシブルディスク、光ディスク（CD-ROM、CD-R、CD-RW、DVD等）、磁気ディスク、磁気テープ、メモリカード等がある。

【0061】その他、プログラムの供給方法としては、インターネットを介して本発明のプログラムをファイル転送によって取得する態様も含まれる。

【0062】また、本発明のプログラムを暗号化してCD-ROM等の記憶媒体に格納してユーザに配布し、所定の条件をクリアしたユーザに対し、インターネットを介して暗号化を解く鍵情報を取得させ、その鍵情報を使用することで暗号化されたプログラムを実行してコンピュータにインストールさせて実現することも可能である。

る。

【0063】また、コンピュータが、読み出したプログラムを実行することによって、前述した実施形態の機能が実現される他、そのプログラムの指示に基づき、コンピュータ上で稼働しているOS等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される。

【0064】さらに、記憶媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によっても前述した実施形態の機能が実現される。

【0065】

【発明の効果】本発明によれば、生成したワнтаイム・パスワードを確実に配送することができ、第三者からの不正アクセスを有効に防御できる安全性の高い通信システムを提供することができ。

【図面の簡単な説明】

【図1】実施形態における無線LANシステムの認証処理のシーケンス図である。

【図2】実施形態における認証サーバの構成を示す図である。

【図3】実施形態における移動端末の構成を示す図である。

【図4】実施形態における別の例による移動端末の構成を示す図である。

【図5】図4の構成を有する移動端末に対する認証処理の一例を示すシーケンス図である。

【図6】従来の無線LANシステムの構成を示す図である。

【図7】IEEE802.11に規定されているWEPアルゴリズムのシーケンス図である。

【図8】WEP暗号化ブロックの構成図である。

【図9】WEP復号化ブロックの構成図である。

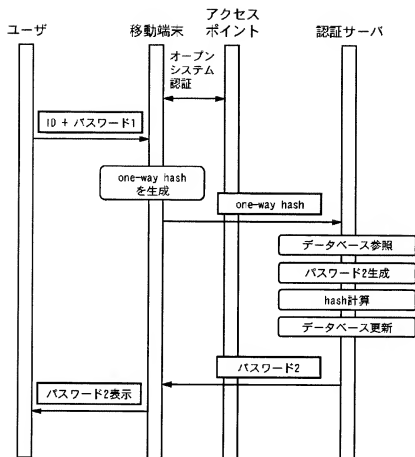
【図10】従来の認証サーバを含む無線LANシステムの構成を示す図である。

【図11】従来の認証サーバによる認証処理のシーケンス図である。

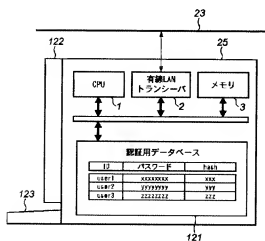
【図12】実施形態におけるユーザ認証による無線LANシステムの構成を示す図である。

【図13】従来のユーザ認証による認証処理のシーケンス図である。

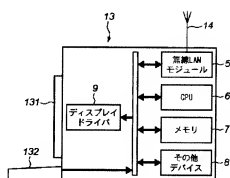
【図1】



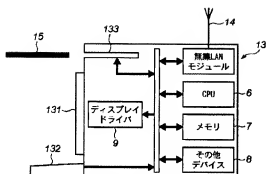
【図2】



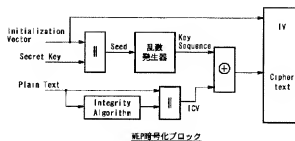
【図3】



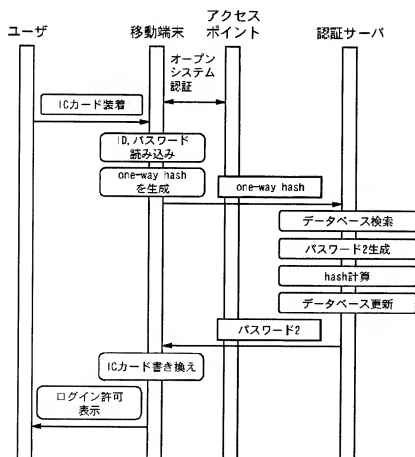
【図4】



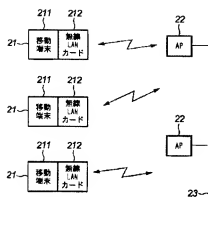
【図8】



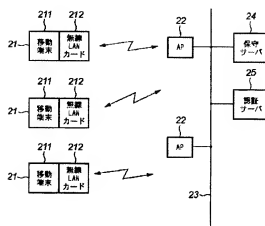
【図5】



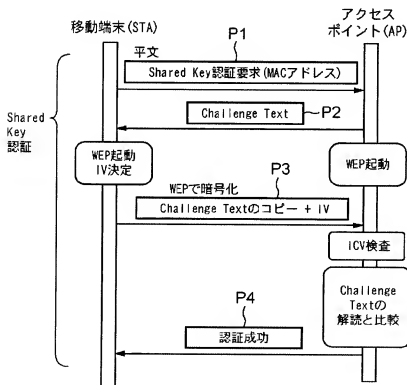
【図6】



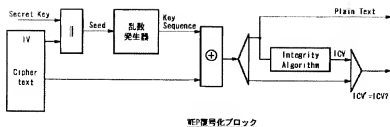
【図10】



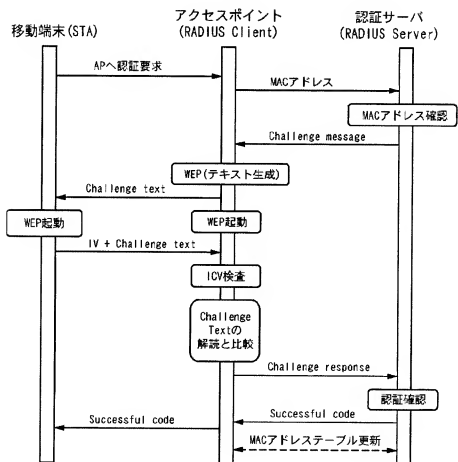
【図7】



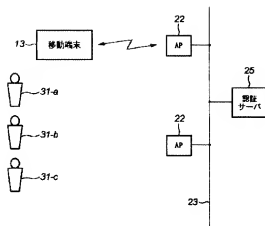
【図9】



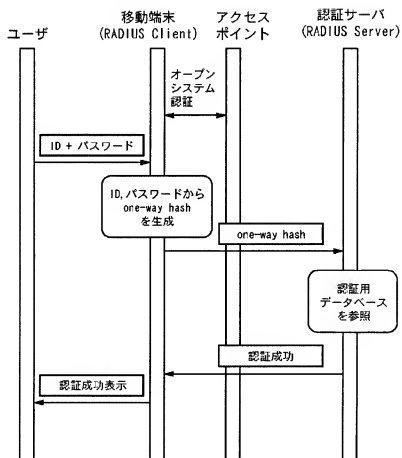
【図11】



【図12】



【図13】



フロントページの続き

F ターム(参考) 5B035 AA13 AA14 BB09 BC00 CA29
5B058 CA02 KA01 KA02 KA04 KA06
KA12 KA31
5B085 AA08 AE03 AE04 AE12 AE23
AE29 BC01 BE01 BE04 BG02
BG07
5J104 AA07 AA16 EA01 EA04 EA22
JA01 JA03 KA01 KA04 MA01
NA02 NA05 NA12 NA33 NA38
NA41 PA01
5K067 AA32 DD17 EE02 EE10 FF02
FF23 HH21 HH23